BiPAC 5200G *RC* Series

802.11g ADSL2+ Firewall Router

User Manual

Version released 2.12.17.0(RE2.C31)3.12.17.0

Last revised : Dec 30, 2011

Table of Contents

Chapter 1: Introduction 1
- Introduction to your Router 1
  - Features 3
  - Application Illustrations 6

Chapter 2: Installing the Router 7
- Package Contents 7
- Hardware Overview 8
  - Front LEDs 8
  - Rear Panel 9
- Cabling 10

Chapter 3: Basic Installation 11
- Network Configuration 12
  - Configuring PC in Windows 7 12
  - Configuring PC in Windows Vista 14
  - Configuring PC in Windows XP 16
  - Configuring PC in Windows 2000 17
  - Configuring PC in Windows 95/98/Me 18
  - Configuring PC in Windows NT4.0 19
- Step by Step Installation 20
- Factory Default Settings 25
- Information from your ISP 26
- Configuring with your Web Browser 27

Chapter 4: Configuration 28
- Quickstart 28
- Interface Setup 34
  - Internet 35
  - LAN 39
  - Wireless 41
- Advanced Setup 45
  - Firewall 45

Routing....46
NAT....48
ADSL....54
Access Management....55
ACL....55
Filter....56
SNMP....60
UPnP....61
DDNS....62
Maintenance....63
Administration....63
Time Zone....64
Firmware....65
SysRestart....66
Diagnostics....67
Status....68
Device Info....68
System Log....70
Statistics....71
Help....74
Appendix: Product Support & Contact....77

Chapter 1: Introduction

Introduction to your Router

Welcome to Billion BiPAC 5200G *RC* Series ADSL2+ Firewall Router. Your Billion router is an “all-in-one” unit, combining an ADSL modem, ADSL router and Ethernet network switch, providing everything you need to get the machines on your network connected to the Internet over your ADSL broadband connection.

This firewall router complies with ADSL2+ standards for worldwide deployment and supports downstream rates of up to 24 Mbps and upstream rates of up to 1 Mbps. It is designed for small office, home office and residential users, enabling even faster speed Internet connections. User can enjoy ADSL services and broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever before.

The product supports PPPoA (RFC 2364 – PPP (Point-to-Point Protocol) over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with ISP. The product also supports VC-based and LLC-based multiplexing.

It is the perfect solution to connect a small group of PCs to a high-speed broadband Internet connection. Multi-users can have high-speed Internet access simultaneously.

This product also serves as an Internet firewall, protecting your network from being accessed by outside users. Not only provide the natural firewall function (Network Address Translation, NAT), it also provides rich firewall features to secure user’s network. All incoming data packets are monitored and filtered. Besides, it can also be configured to block internal users from accessing to the Internet.

The product provides two levels of security support. First, it masks LAN users’ IP addresses which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. Secondly, it can block and redirect certain ports to limit the services that outside users can access. For example, to ensure that games and other Internet applications will run properly, user can open some specific ports for outside users to access internal services in network.

Integrated DHCP (Dynamic Host Control Protocol) services, client and server, allow multiple users to get their IP addresses automatically on boot up from the product. Simply set local machines as a DHCP client to accept a dynamically assigned IP address from DHCP server . Each time local machine is powered up; the router will recognize it and assign an IP address to instantly connect it to the LAN.

For advanced users, Virtual Service function allows the product to provide limited visibility to local machines with specific services for outside users. An ISP (Internet Service Providers) provided IP address can be set to the product and then specific services can be rerouted to specific computers on the local network. For instance, a dedicated web server can be connected to the Internet via the product and then incoming requests for HTML that are received by the product can be rerouted to the dedicated local web server, even though the server now has a different IP address. In this example, the product is on the Internet and vulnerable to attacks, but the server is protected.

Virtual Server can also be used to re-task services to multiple servers. For instance, the product can be set to allow separated FTP, Web, and Multiplayer game servers to share the same Internet-visible IP address while still protecting the servers and LAN users from hackers.

Features

ADSL Multi-Mode Standard

Supports downstream rates of up to 24 Mbps and upstream rates of up to 1 Mbps. It also supports rate management that allows ADSL subscribers to select an Internet access speed suiting their needs and budgets. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt(G.992.1); G.lite(G992.2)), G.hs (G994.1), G.dmt.bis (G.992.3), G.dmt.bisplus (G.992.5)). The Annex A and B are supported in different H/W platforms.

802.11g Wi-Fi

With built-in 802.11g access point for extending the communication media to WLAN while providing the WEP, WPA and WPA2 for securing your wireless networks.

Fast Ethernet Switch

A 4-port 10/100Mbps fast Ethernet switch is built in with automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports. An Ethernet straight or crossover cable can be used directly for auto detection.

Multi-Protocol to Establish a Connection

It supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation overATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.

Quick Installation Wizard

It supports a WEB GUI page to install this device quickly. With this wizard, end users can enter the information easily which they get from their ISP, then surf the Internet immediately.

Universal Plug and Play (UPnP) and UPnP NAT Traversal

This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.

Network Address Translation (NAT)

Allows multi-users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateway (ALG) are supported such as

web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.

Domain Name System (DNS) Relay

It provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router's IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in the outside network.

Dynamic Domain Name System (DDNS)

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply for an account from a DDNS service like http://www.dyndns.org/. More than 5 DDNS servers are supported.

Virtual Server

Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it. For example, a user can assign a PC in the LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse inside web servers directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.

Dynamic Host Configuration Protocol (DHCP) Client and Server

In the WAN site, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. In the LAN site, the DHCP server can allocate a range of client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.

RIP1/2 Routing

It has the routing capability that supports RIP1/2 routing protocol.

Simple Network Management Protocol (SNMP)

It is an easy way to remotely manage the router via SNMP.

Web based GUI

It supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.

Firmware Upgradeable

Device can be upgraded to the latest firmware through the WEB based GUI.

Firewall

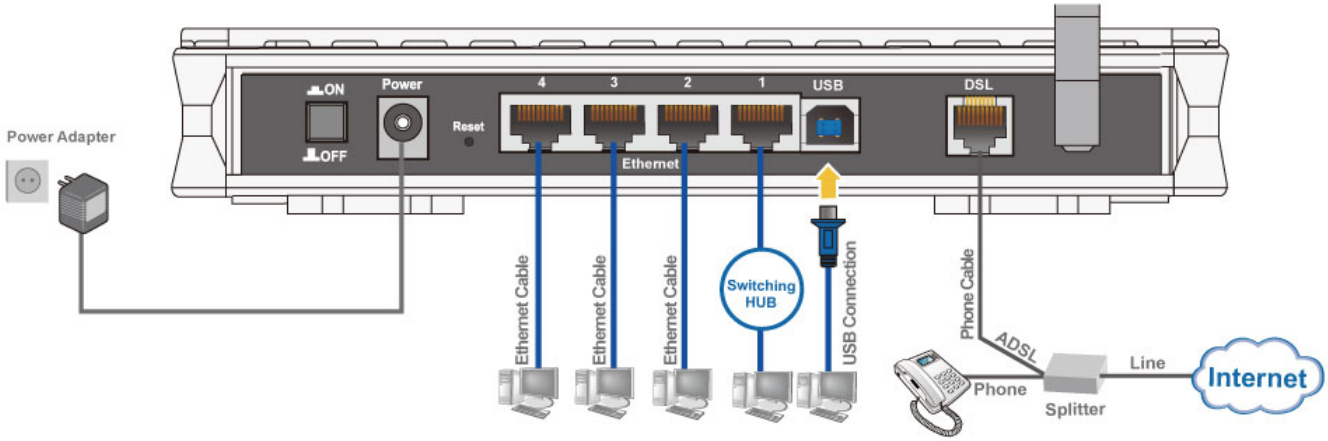
Supports simple firewall with NAT technology and provides option for blocking access from Internet, like Telnet, FTP, WEB, SNMP and IGMP.

PPP over Ethernet (PPPoE)

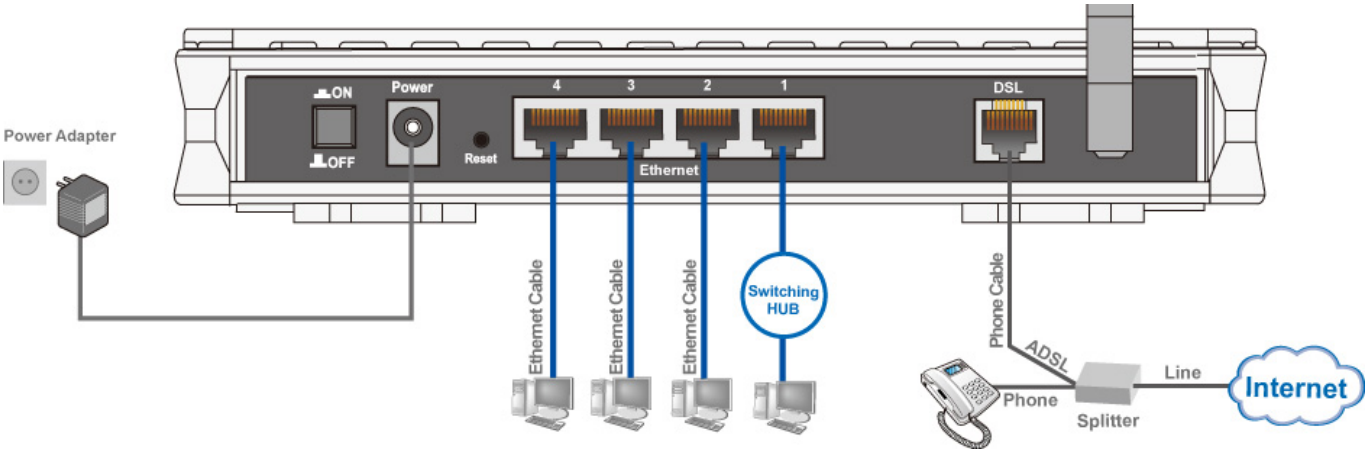
Provides embedded PPPoE client function to establish a connection. Users can get greater access speed without changing the operation concept, sharing the same ISP account and paying for one access account. No PPPoE client software is required for local computer. The Automatic Reconnect and Disconnect Timeout (Idle Timer) functions are provided, too.

Application Illustrations

5210G *RC*



5200G *RC* / 5200G *RD*



Chapter 2: Installing the Router

Important Note for Using this Router

Warning

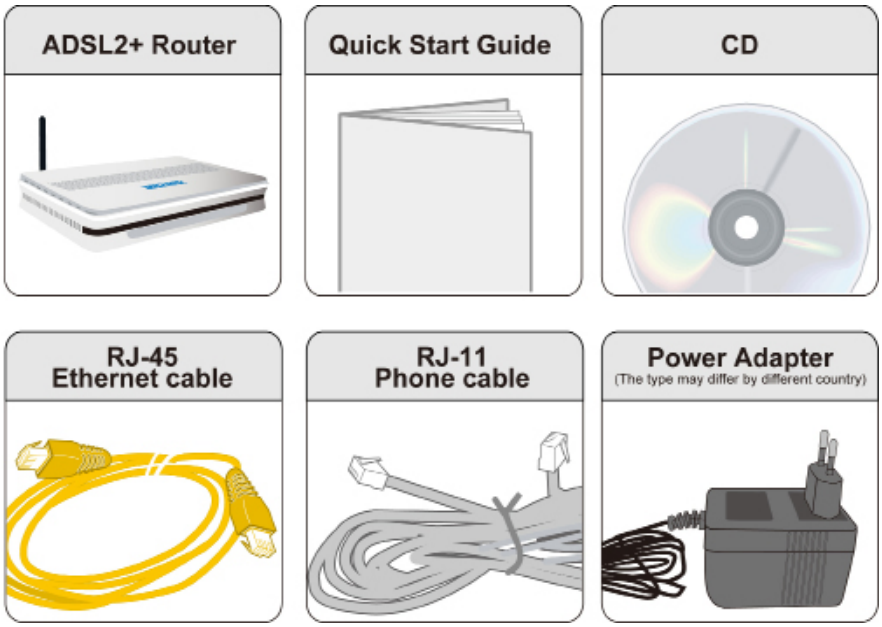
- Do not use this router in a high humidity or high temperature environment.
- Do not apply the same power source for this router to other types of equipments.
- Do not open or repair the case yourself. If the device becomes too hot, turn it off immediately and have it repaired at a qualified service center.
- Avoid using this product and all its accessories outdoor.

Attention

- Place the router on a stable surface.
- Only use the power adapter that comes with the package. Using a different voltage rating power adapter may damage the router.

Package Contents

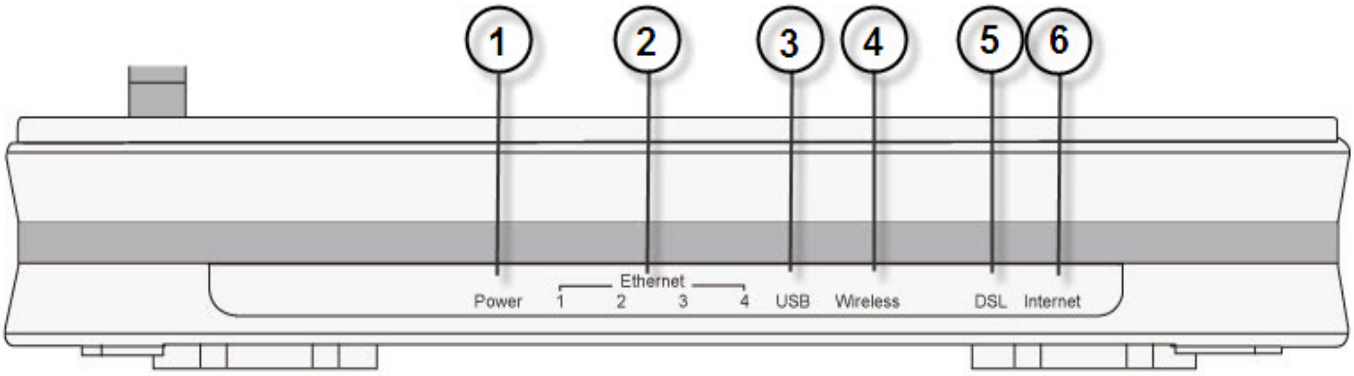
- **BiPAC ADSL2+ Firewall Router**
- **CD containing the online manual**
- **RJ-11 ADSL/telephone Cable**
- **Ethernet (RJ-45) Cable**
- **Power adapter**
- **USB cable (only for BiPAC 5210G *RC*)**
- **Quick Start Guide**
- **Micro-filter / Splitter (optional)**



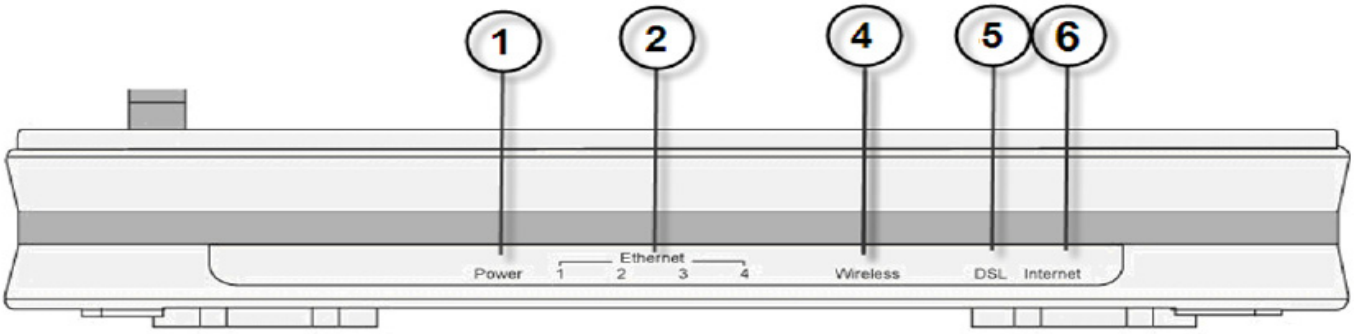
Hardware Overview

Front LEDs

5210G *RC*



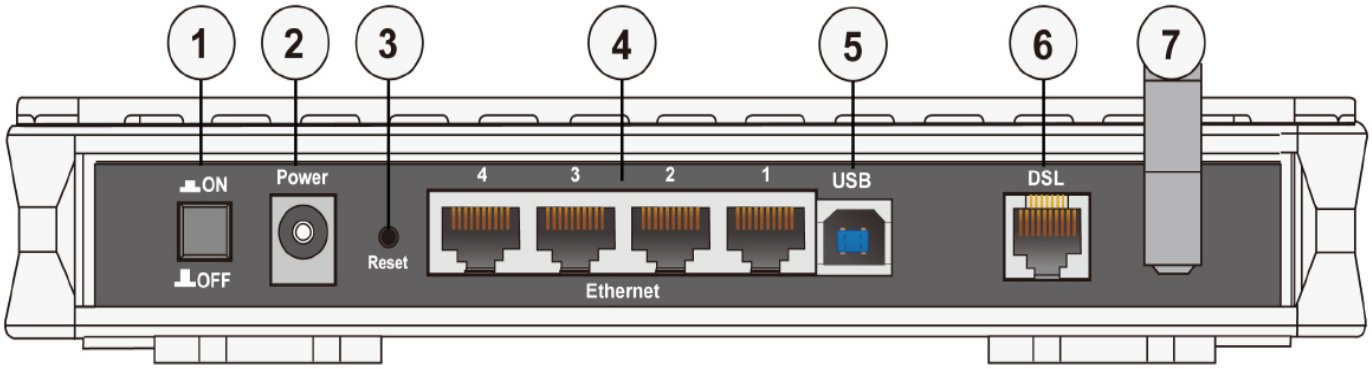
5200G *RC* / 5200G *RD*



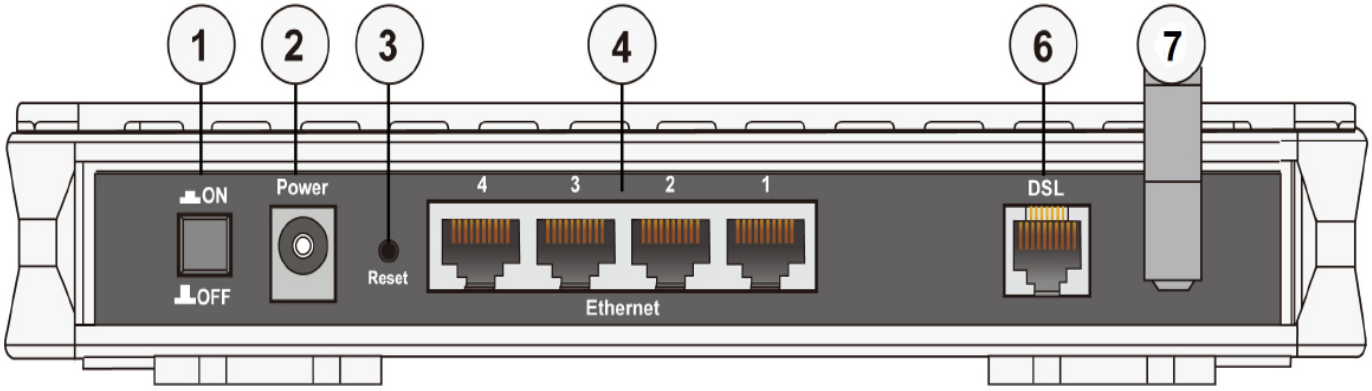
LED		Meaning
1	**Power**	Lit red when power is ON. Lit green when the system is ready.
2	**Ethernet**	Lit when connected to an Ethernet device. Lit green when the speed of transmission hits 10/100Mbps. Blink when data is being Transmitted / Received.
3	**USB (Only for 5210G *RC*)**	Lit green when the router is connected to a USB device. Flash when data is received / transmitted.
4	**Wireless**	Lit green when a wireless connection is established. Blink when data is being sent / received.
5	**DSL**	Lit Green when the device is successfully connected to an ADSL DSLAM. (“line sync”).
6	**Internet**	Lit red when WAN port fails to get IP address. Lit green when WAN port gets IP address successfully.

Rear Panel

5210G *RC*



5200G *RC* / 5200G *RD*



		Meaning
1	**Power Switch**	Power ON / OFF switch.
2	**Power adapter**	Connect with the supplied power adapter.
3	**Reset**	When the device power is on, press to reset or to restore its factory default setting. Press 1-3 seconds to reset the device. Press 6 seconds and above to restore the device factory default setting.
4	**Ethernet**	Connect to a home / office network device (eg. PC) of 100Mbps or 10Mbps with the supplied UTP Ethernet cable (CAT-5).
5	**USB (Only for 5210G *RC*)**	User can connect to PC using an alternative USB cable through this port.
6	**DSL (Line)**	Connect to a telephone network / ADSL using the provided RJ-11 cable.
7	**Antenna**	Connect the antenna to this port.

Cabling

One of the most common causes of problem is bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front panel of your router is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify if you are using the proper cables.

Make sure that all devices (e.g. telephones, fax machines, analogue modems) connected to the same telephone line as your router have a line filter connected between them and the wall outlet (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and that all line filters are correctly installed in a right way. If line filter is not installed and connected properly, it may cause problem to your ADSL connection or may result in frequent disconnections.

Chapter 3: Basic Installation

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 7/98/NT/2000/XP/Me/Vista, etc. The product provides an easy and user-friendly interface for configuration.

Please check your PC network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.1.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

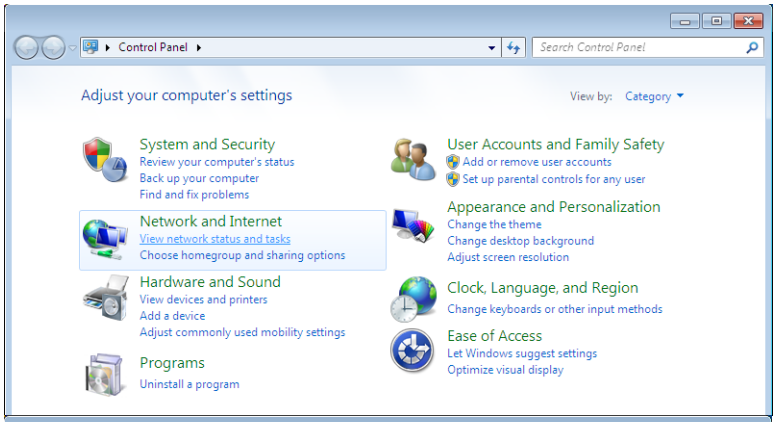
Please follow the following steps to configure your PC network environment.

NOTE: Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

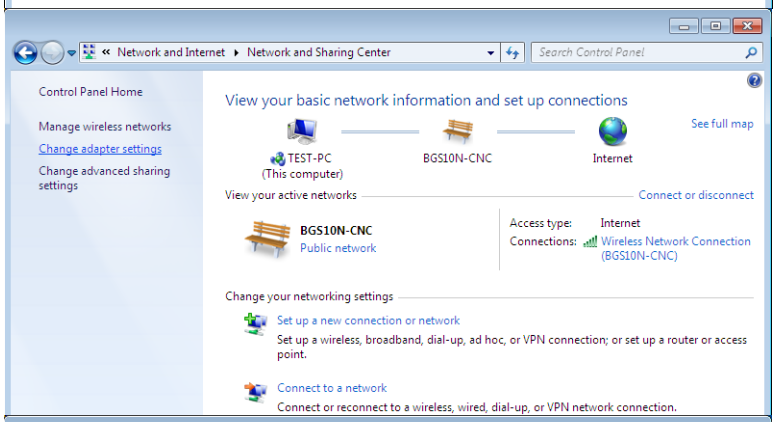
Network Configuration

Configuring PC in Windows 7

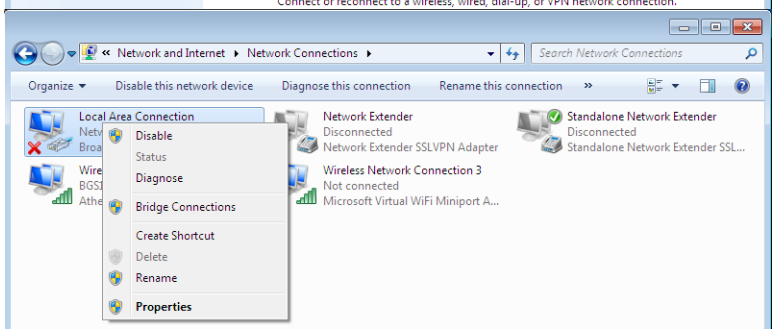
1. Go to Start. Click on Control Panel.
2. Then click on Network and Internet.



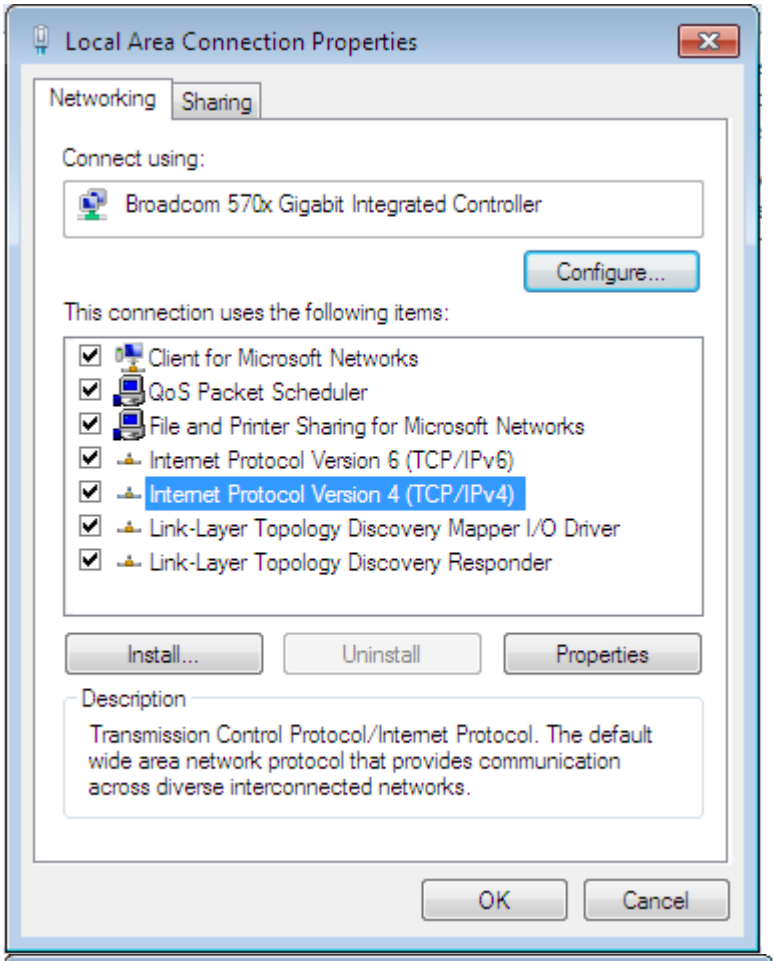
3. When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.



4. Select the Local Area Connection, and right click the icon to select Properties.

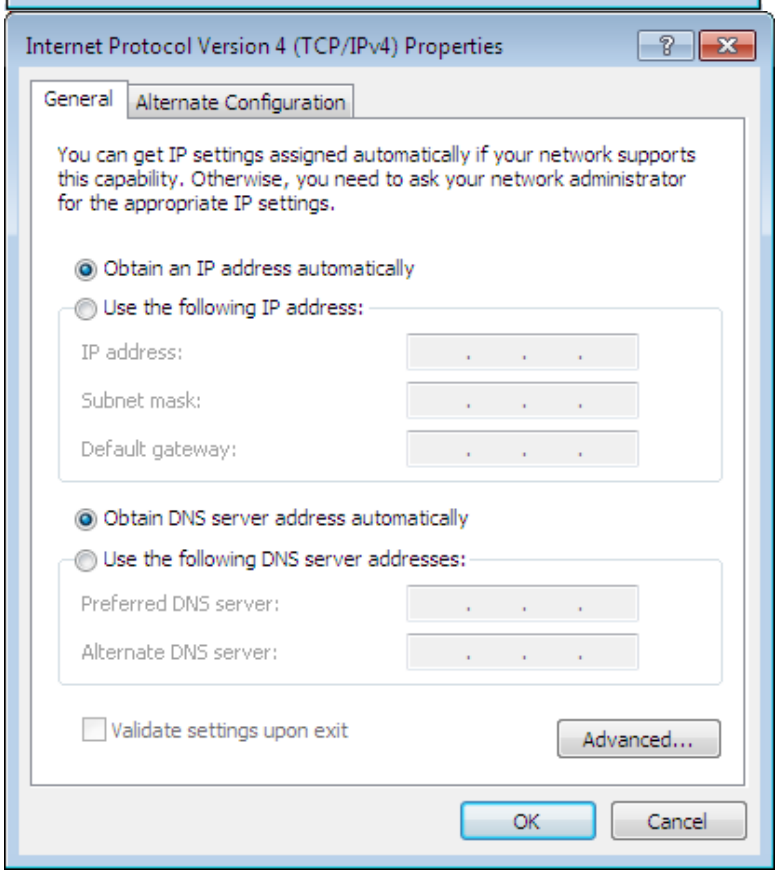


5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



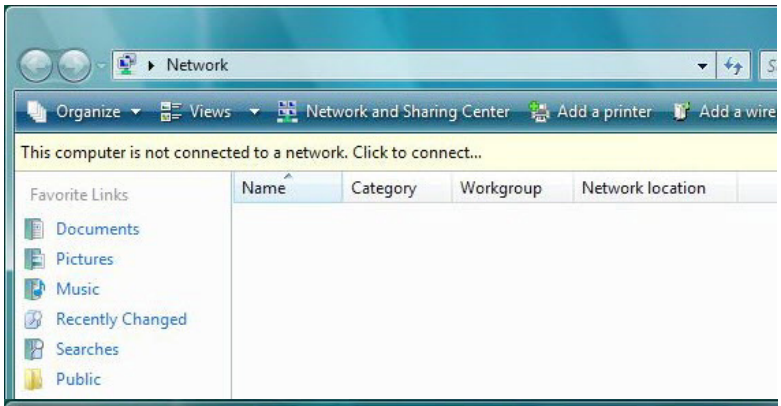
6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.

7. Click OK again in the Local Area Connection Properties window to apply the new configuration.

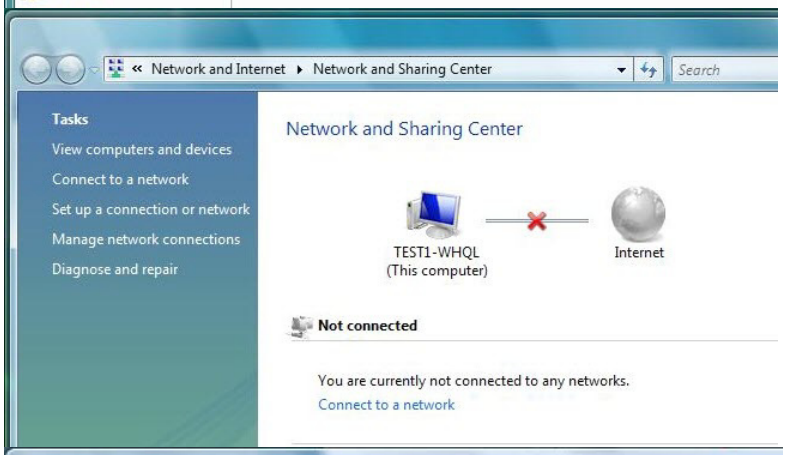


Configuring PC in Windows Vista

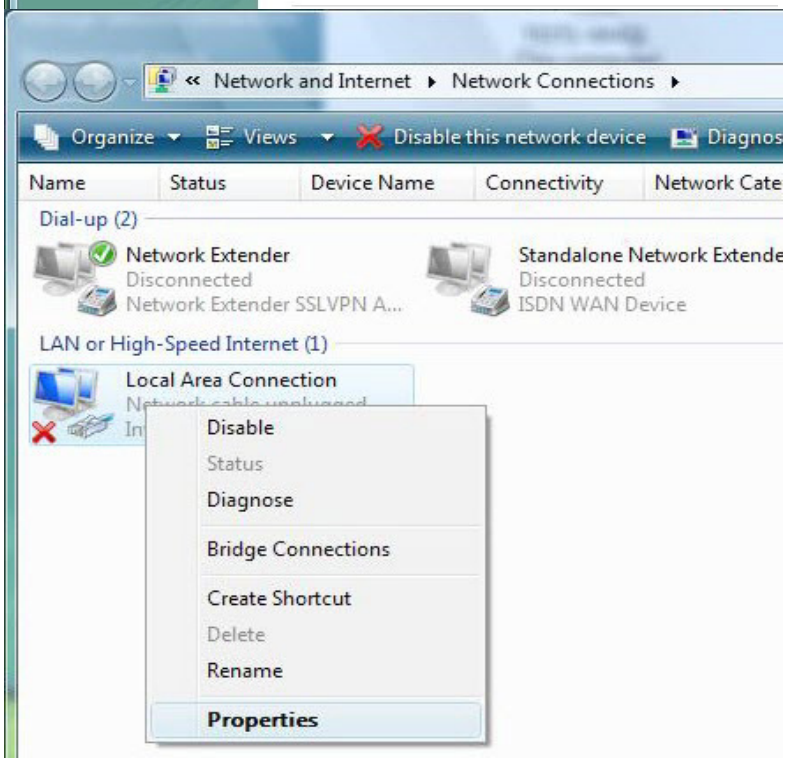
1. Go to Start. Click on Network.
2. Then click on Network and Sharing Center at the top bar.



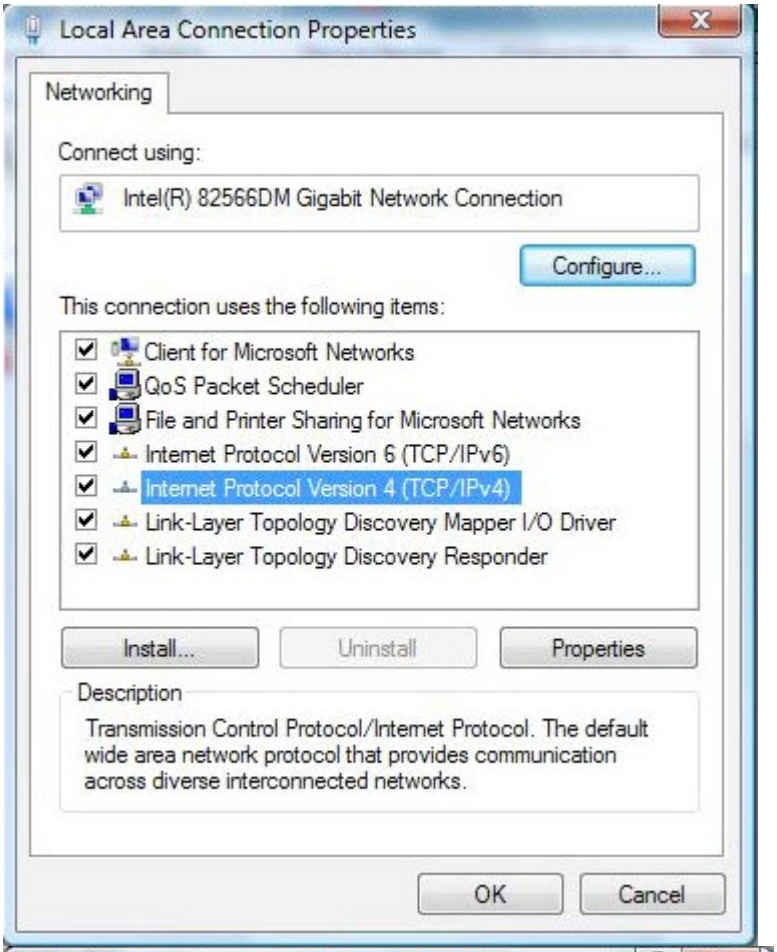
3. When the Network and Sharing Center window pops up, select and click on Manage network connetions on the left window column.



4. Select the Local Area Connection, and right click the icon to select Properties.

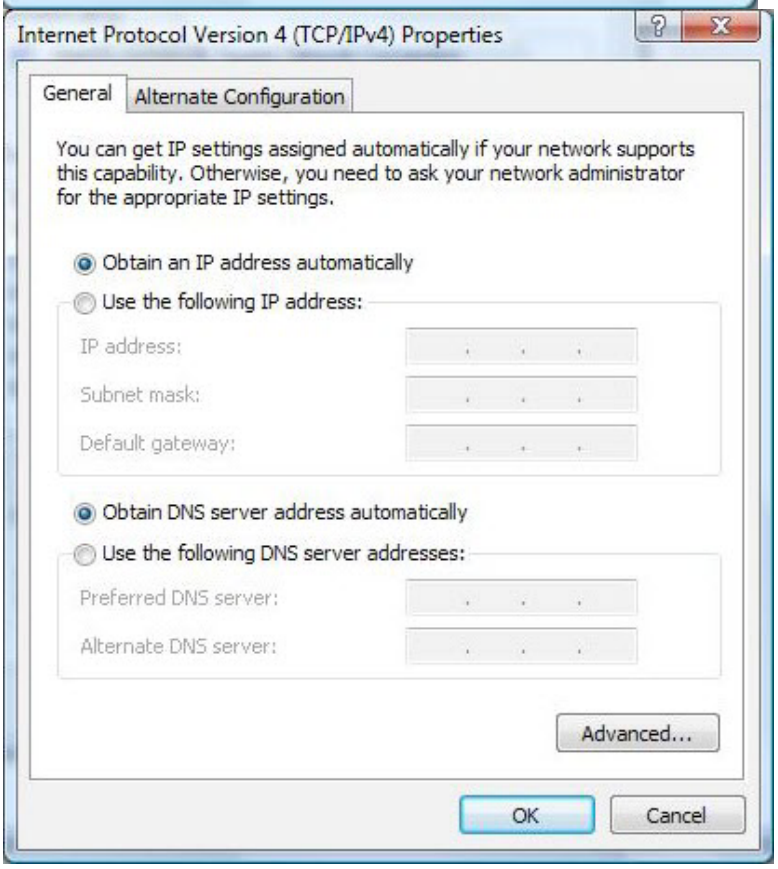


5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.

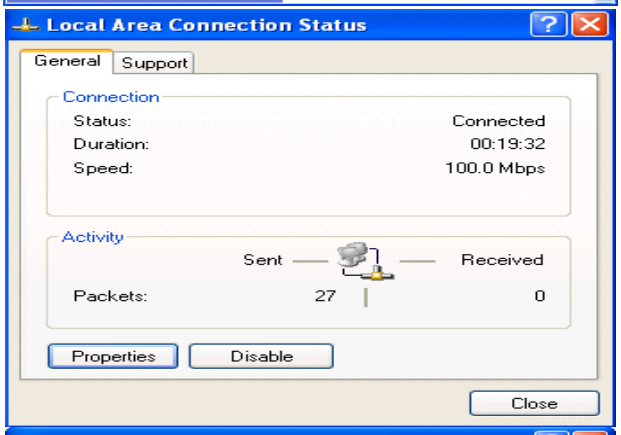
7. Click OK again in the Local Area Connection Properties window to apply the new configuration.



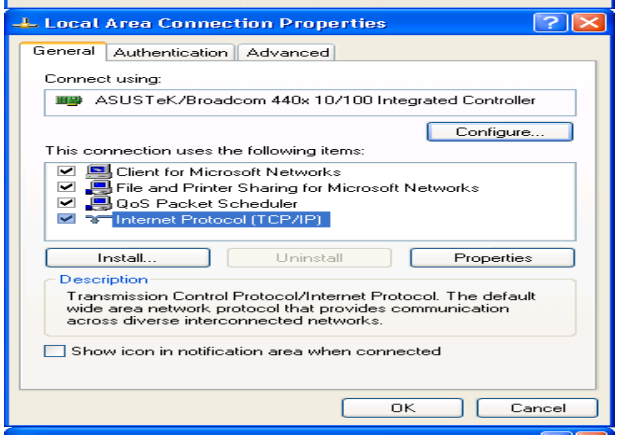
Configuring PC in Windows XP

1. Go to Start > Control Panel (in Classic View). In the Control Panel, double-click on Network Connections
2. Double-click Local Area Connection.

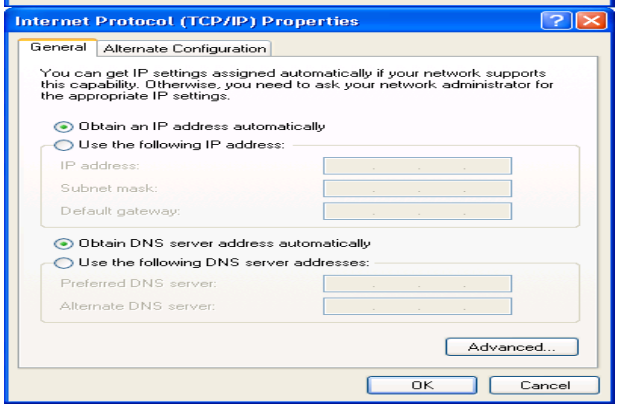
3. In the Local Area Connection Status window, click Properties.



4. Select Internet Protocol (TCP/IP) and click Properties.

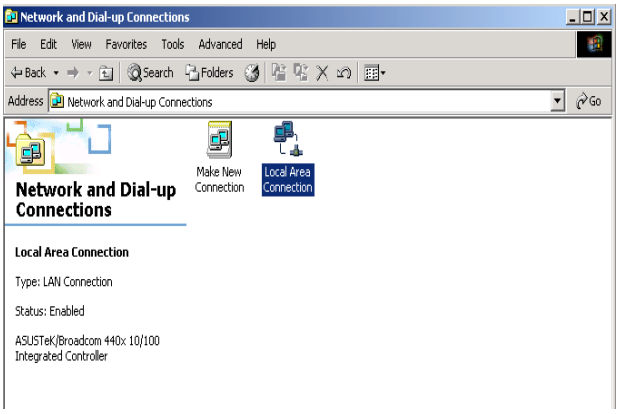


5. Select the Obtain an IP address autmatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

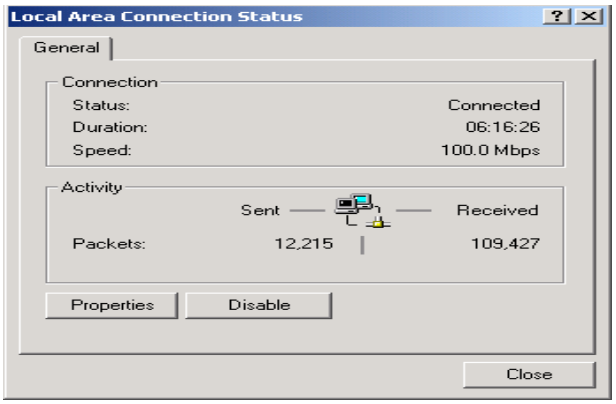


Configuring PC in Windows 2000

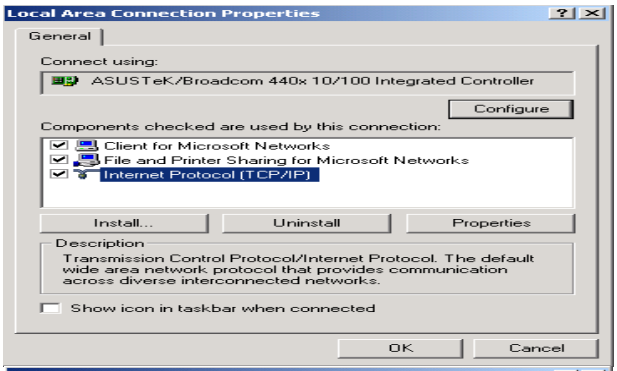
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and Dial-up Connections.
2. Double-click Local Area Connection.



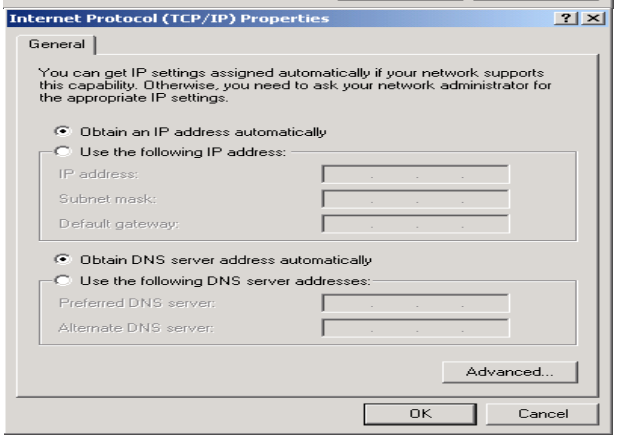
3. In the Local Area Connection Status window click Properties.



4. Select Internet Protocol (TCP/IP) and click Properties.

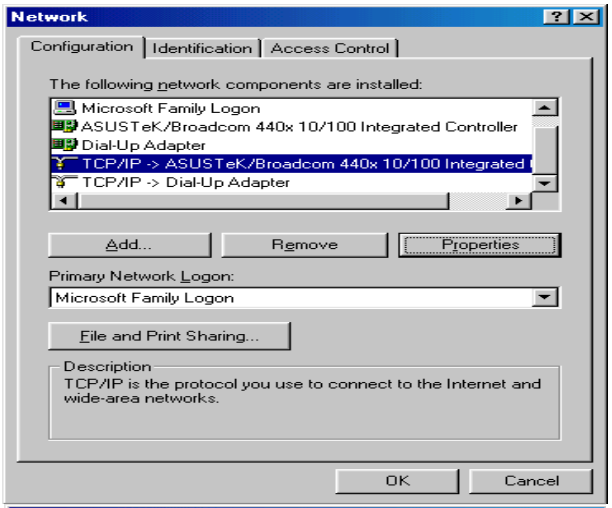


5. Select the Obtain an IP address autmatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

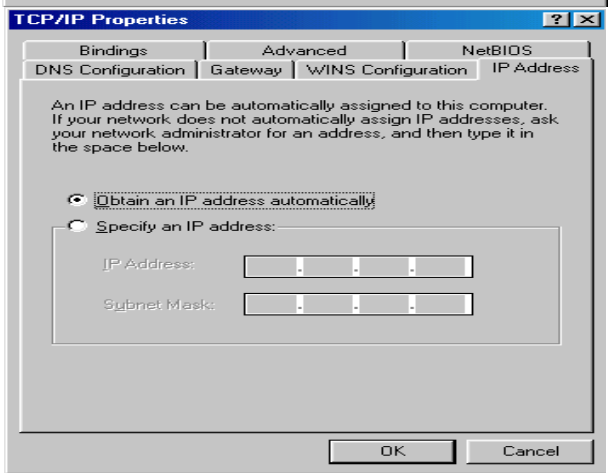


Configuring PC in Windows 95/98/Me

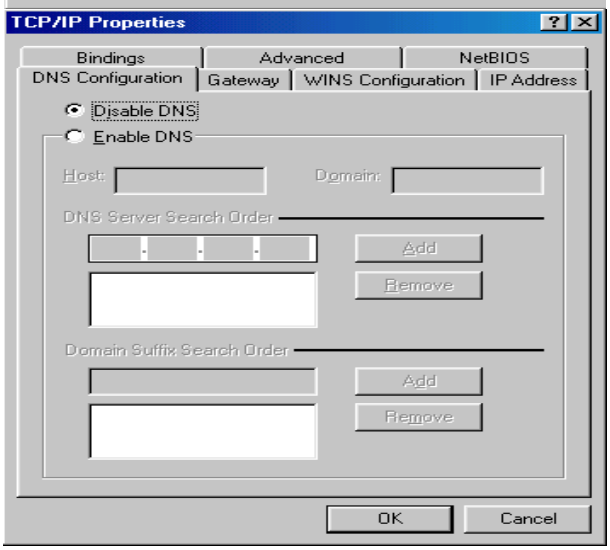
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Configuration tab.
2. Select TCP/IP > NE2000 Compatible, or the name of your Network Interface Card (NIC) in your PC.



3. Select the Obtain an IP address autmatically radio button.

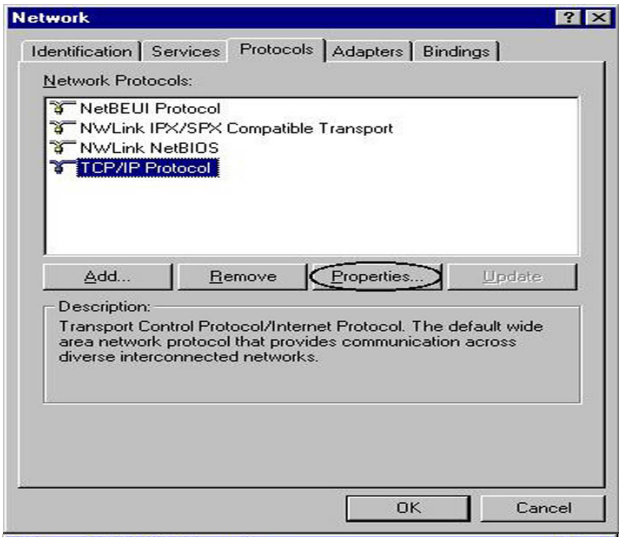


4. Then select the DNS Configurationtab.
5. Select the Disable DNS radio button and click OK to finish the configuration.

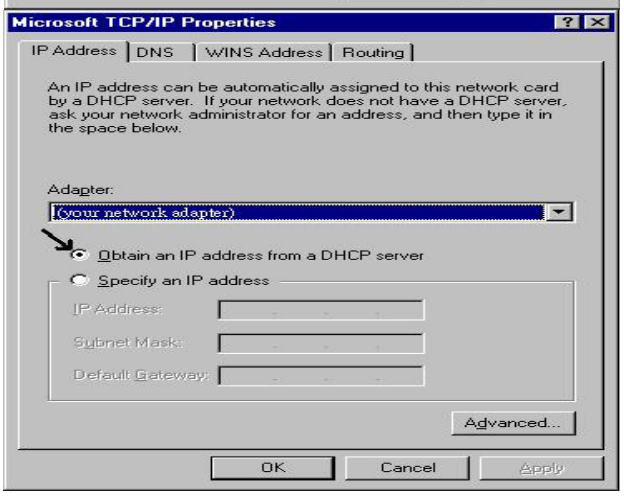


Configuring PC in Windows NT4.0

1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.
2. Select TCP/IP Protocol and click Proerties.



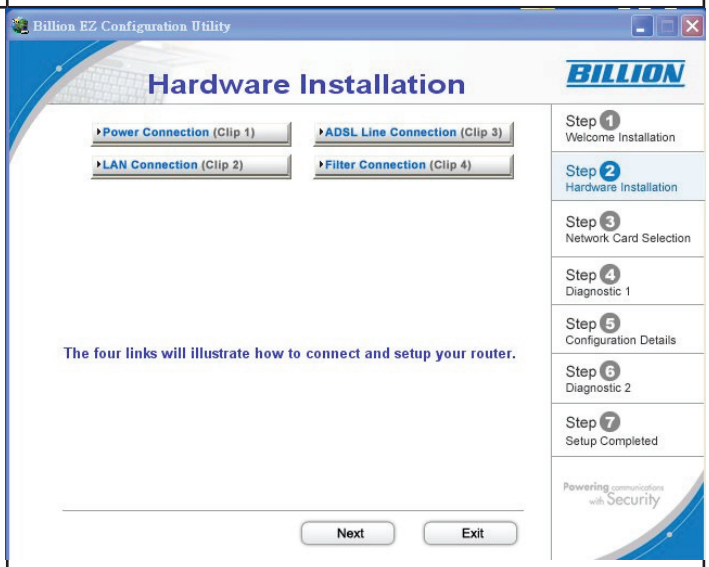
3. Select the Obtain an IP address from a DHCP server radio button and click OK.



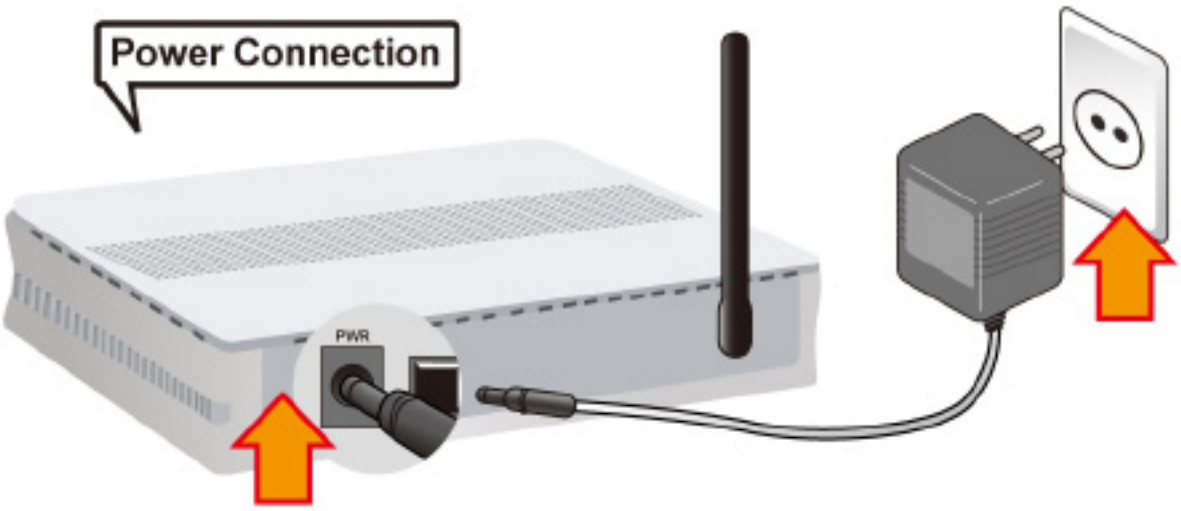
Step by Step Installation

1. Insert the CD into the CD-ROM drive.
2. Execute the Windows Utility.
3. When the Welcome screen appears, click on Next.

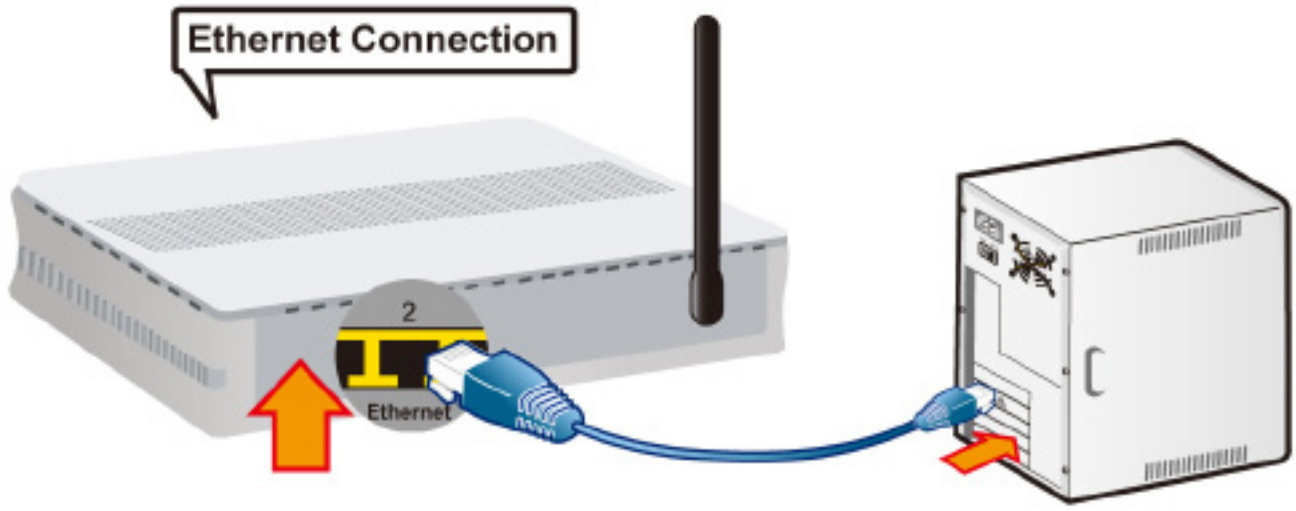
4. When the Hardware Installation wizard appears, you will notice that there are 4 diferent links on the screen. Click on each of them one by one and follow the instructions to complete the installation process.



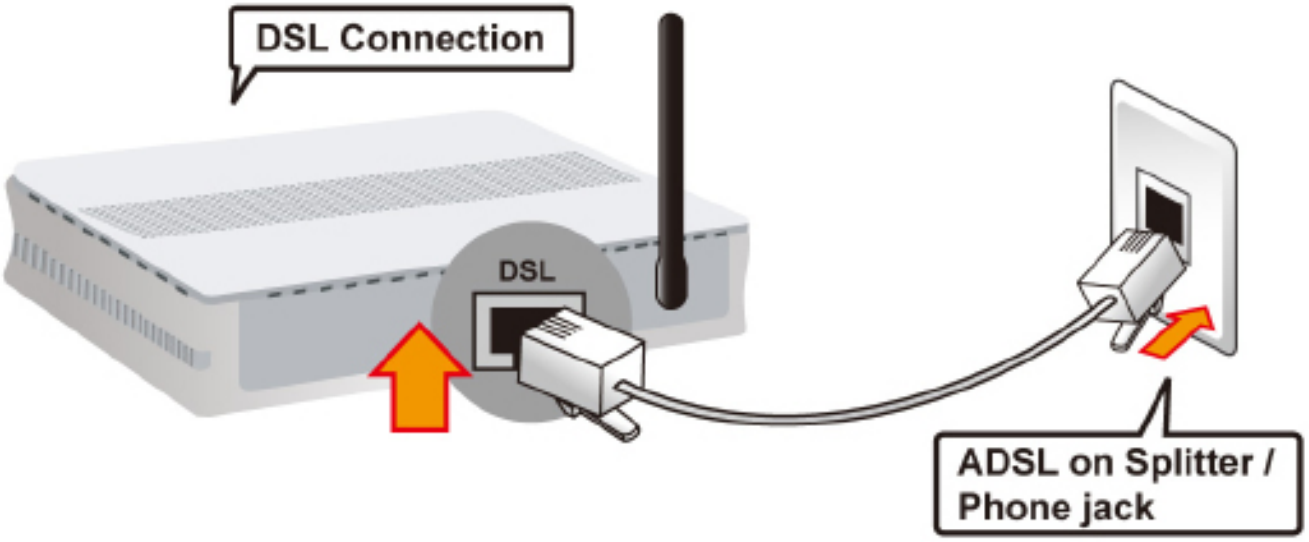
4.1 Power Connection



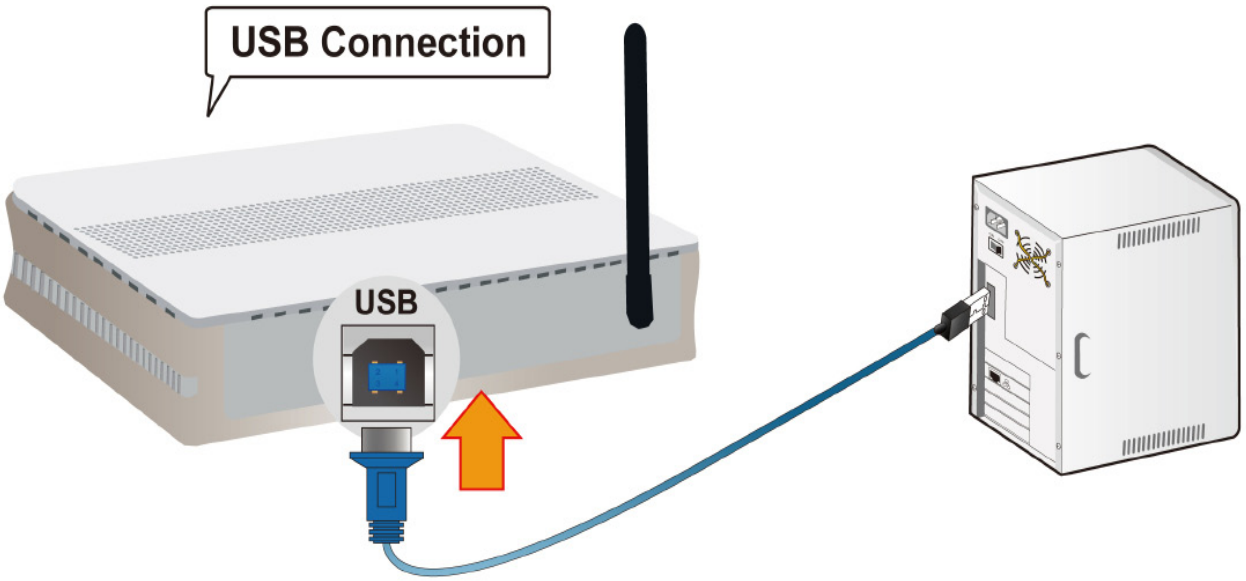
4.2 LAN Connection



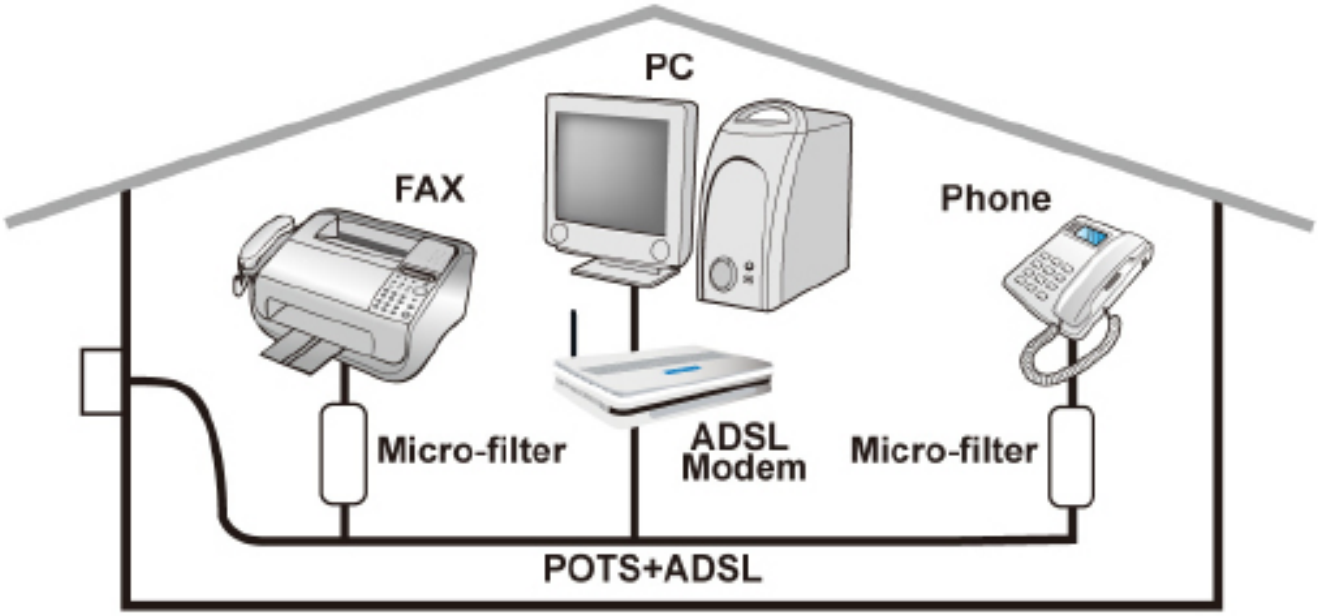
4.3 ADSL Connection



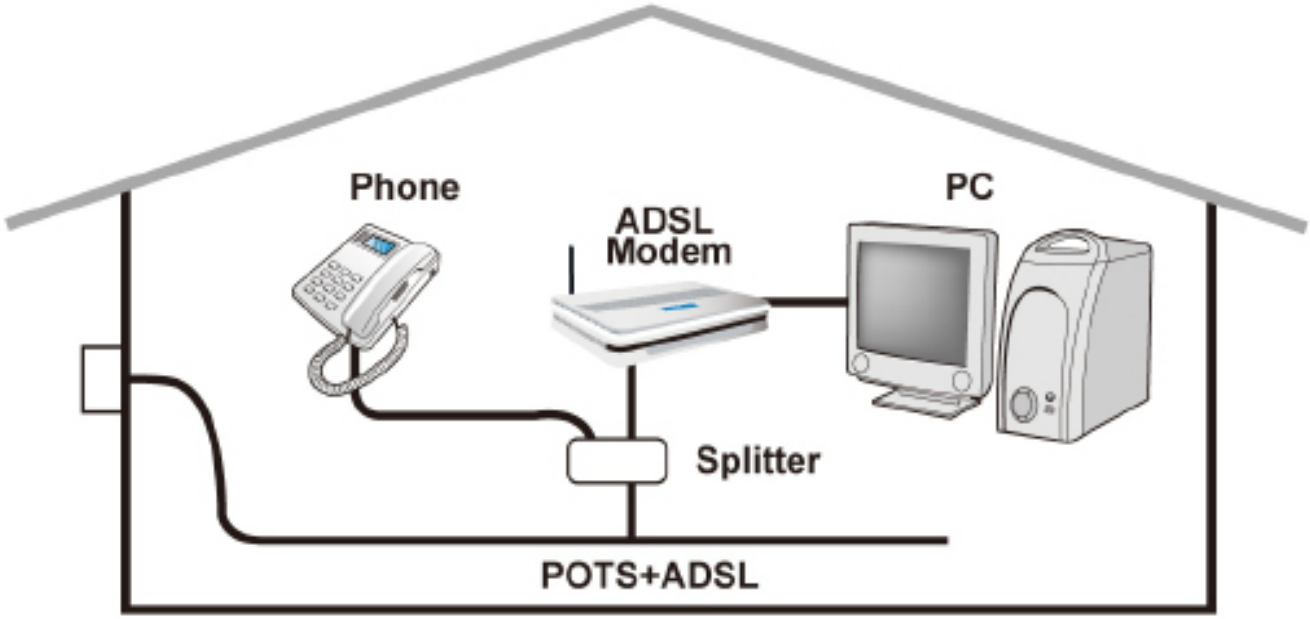
4.4 USB Connection (Only for 5210G ***RC***)



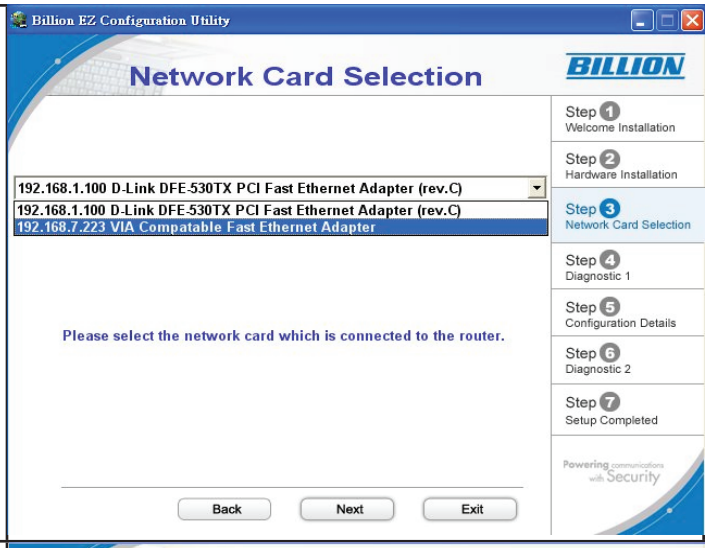
4.5 Micro-Filter Connection



4.6 Splitter Connection

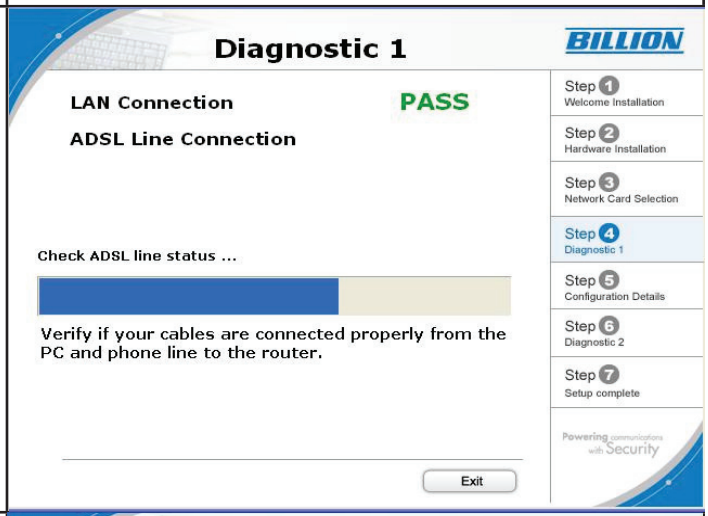


5. When Hardware Installation is complete, click Next to proceed to Network Card Seletion step.

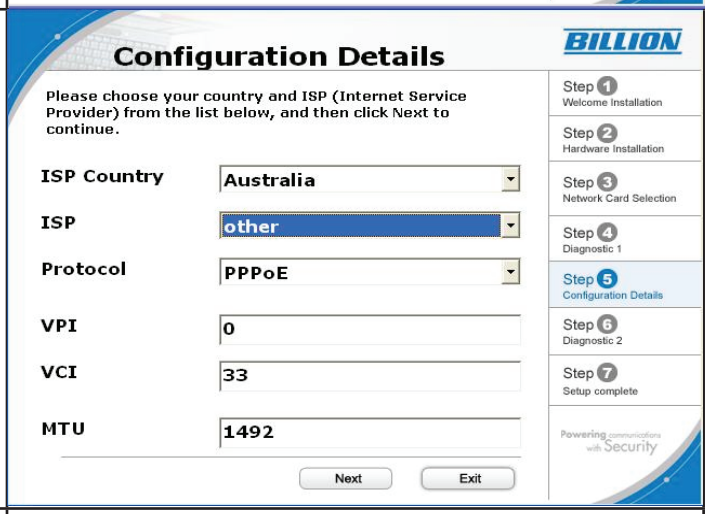


6. Diagnostic Screen: If the connection fails, the FAIL status will be displayed on the screen. Check the connection of the router to see if it is correct.

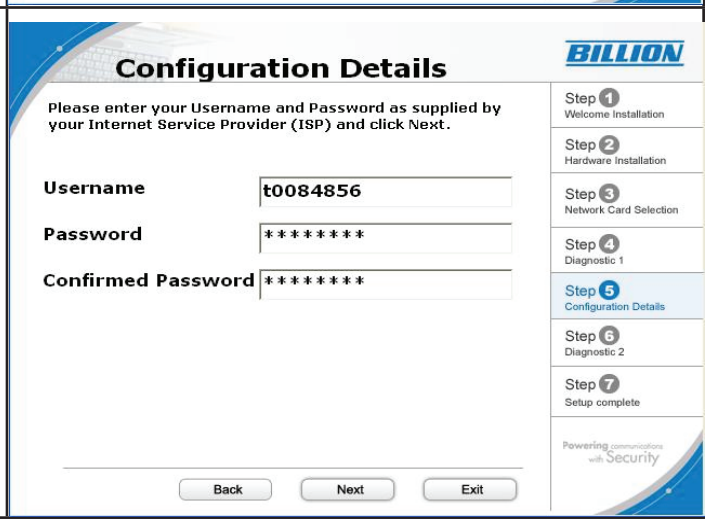
7. When diagnostic test is passed, click Next to proceed to configuration Detail wizard.



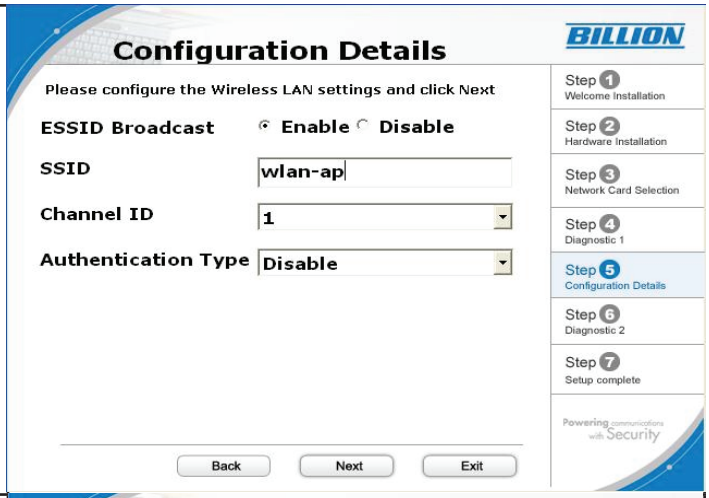
8. Set up the detail setting for VCI, VPI and MTU.



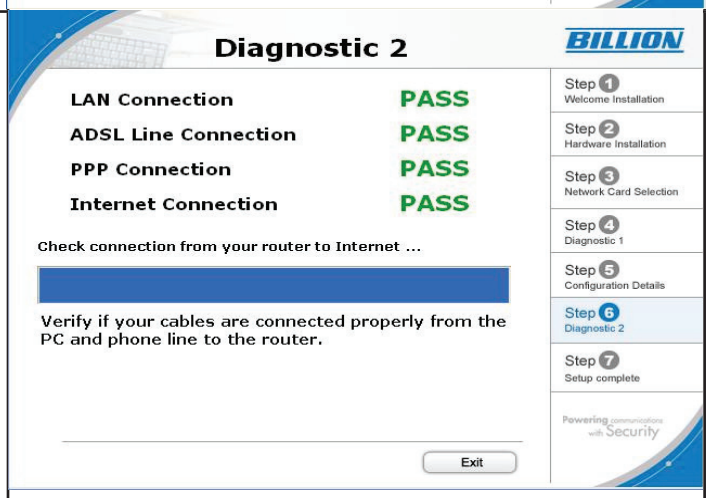
9. Please enter the Username and password as supplied by your ISP (Internet Service Prvider) then click Next.



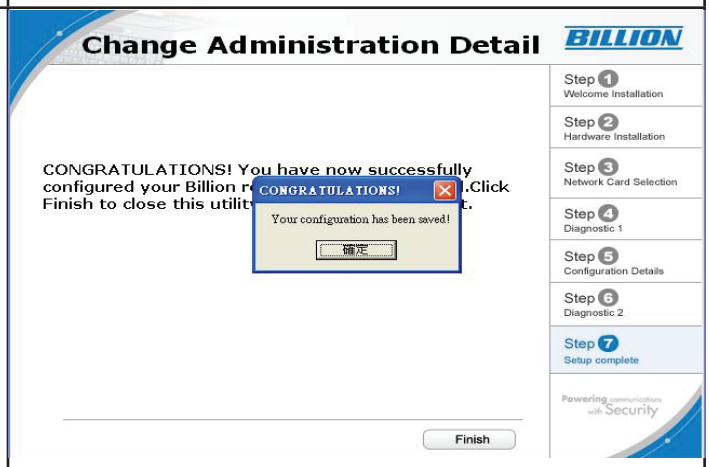
10. Configure the Wireless LAN setting. Then click Next.



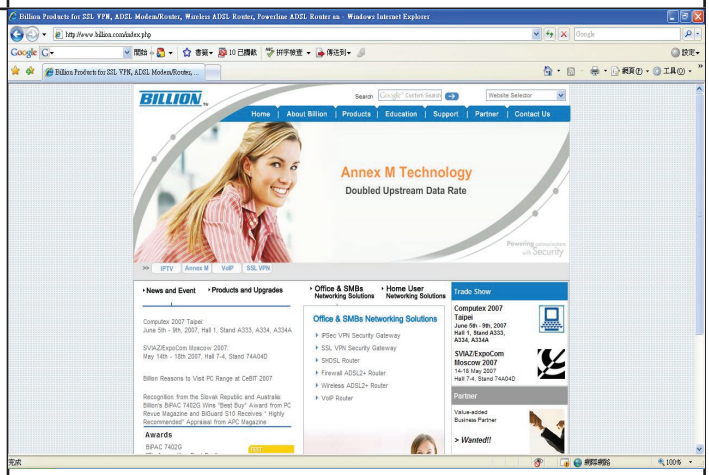
11. Click Next to run a diagnostic test on all your configurations and connections.



12. When all diagnostic tests are passed, you have completed the installation and can conect to the internet.



13. When the installation procedure is complete, your IE browser will be initiated autmatically.



Factory Default Settings

Before configuring your router, you need to know the following default settings.

Web Interface (Username and Password)

- Username: admin
- Password: admin

The default username and password are “**admin**” and “**admin**” respectively.

Device LAN IP settings

- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0

ISP setting in WAN site

- PPPoE

DHCP server

- DHCP server is enabled.
- Start IP Address: 192.168.1.100
- IP pool counts: 100

LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown in the table.

LAN Port		WAN Port
IP address	192.168.1.254	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP (Obtain an IP Address Automatically, Static IP (Fixed IP Address) or PPPoE.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE(RFC2516)	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoA(RFC2684)	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
MPoA(RFC1483/ RFC2684)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA(RFC1577)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
Pure Bridge	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.

Configuring with your Web Browser

Open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click “Go”, a user name and password window prompt will appear. The default username and password are “admin” and “admin” respectively. (See Figure 3.14)

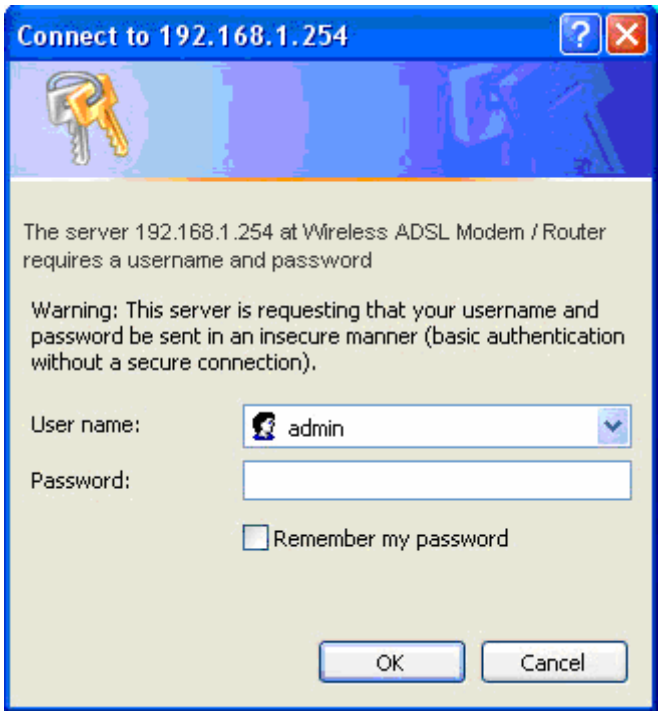


Figure 3.14: User name & Password Prompt Window

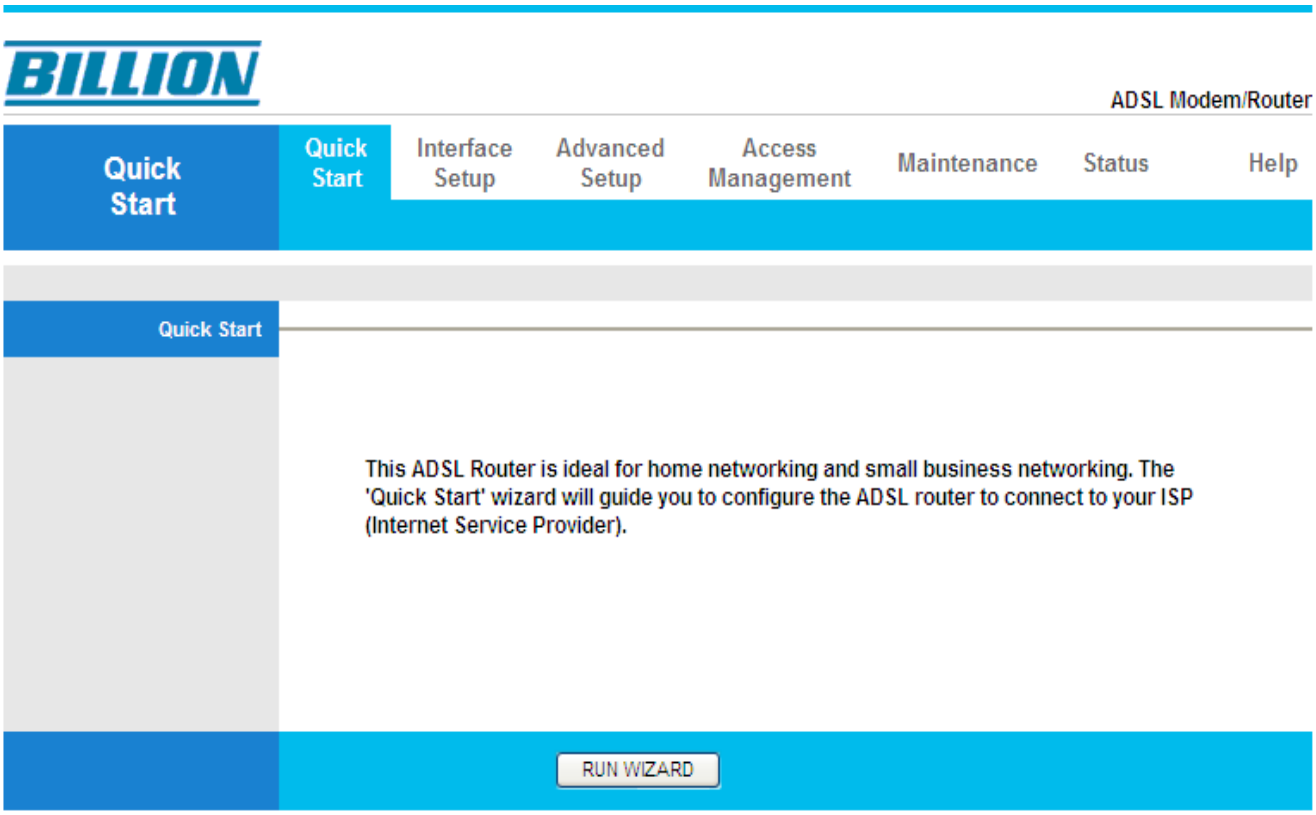
Congratulations! You are now successfully logon to the BiPAC Firewall Router!

Chapter 4: Configuration

At the configuration homepage, the top navigation column provides you the link to each configuration page. The category of each configuration page is listed as below.

- **Quickstart**
- **Interface Setup**
- **Advanced Setup**
- **Access Management**
- **Maintenance**
- **Status**
- **Help**

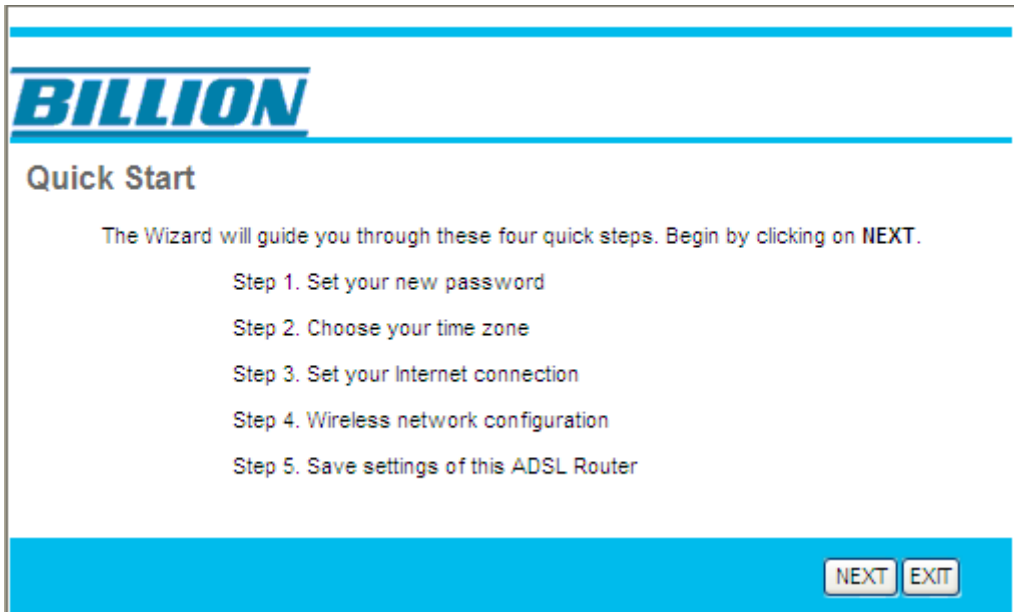
Quickstart



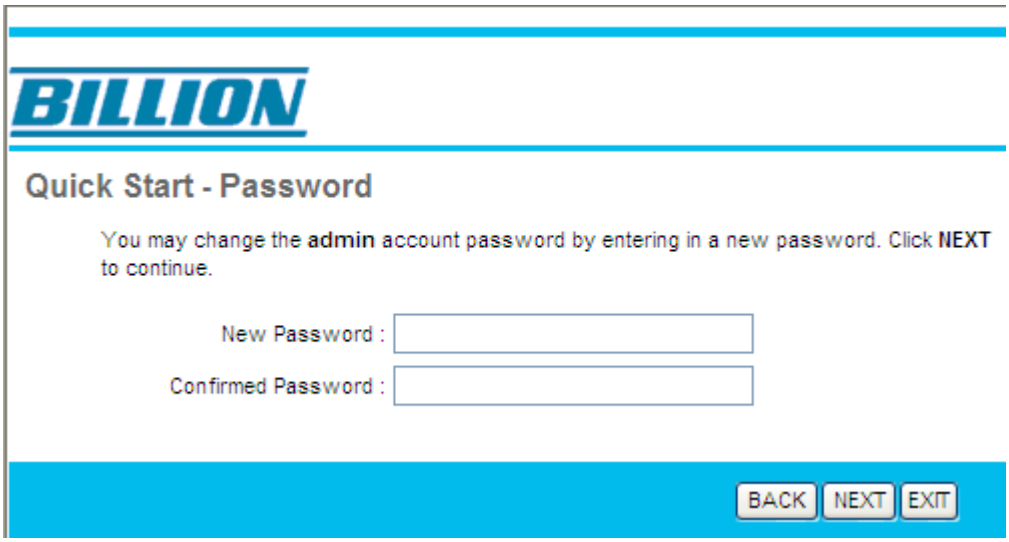
For detailed instructions on configuring WAN settings, see the Interface Setup section of this manual.

The Quick Start Wizard is a useful and easy utility to help setup the device to connect to your ISP (Internet Service Provider) with only a few steps required. It will guide you step by step to configure the password, time zone, and WAN settings of your device. The Quick Start Wizard is a helpful guide for first time users.

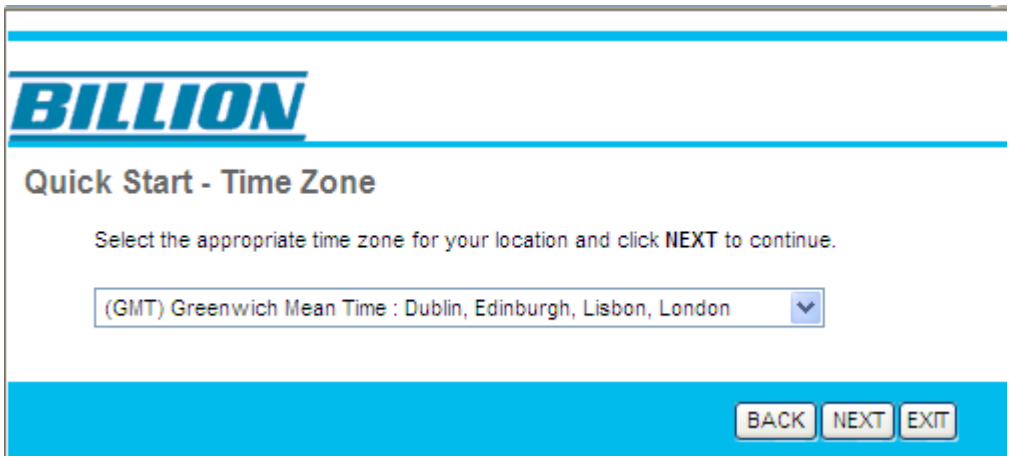
Click **RUN WIZARD,** then the Quick Start Wizard window appears, follow it step by step to configure the Quick Start.



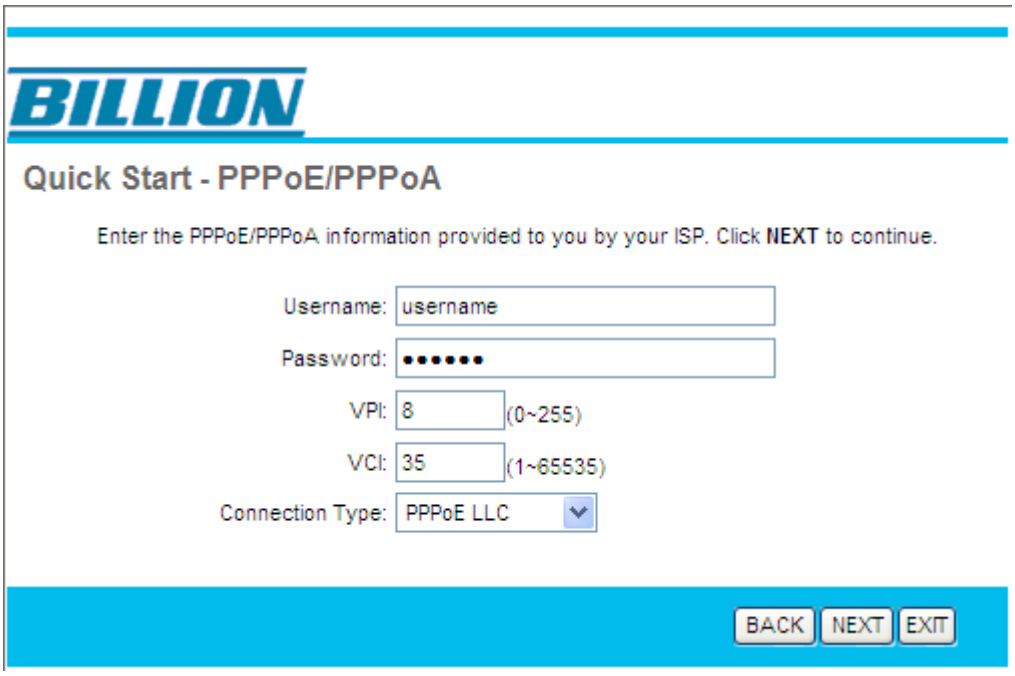
Step 1: Setup your new password. Then click Next.



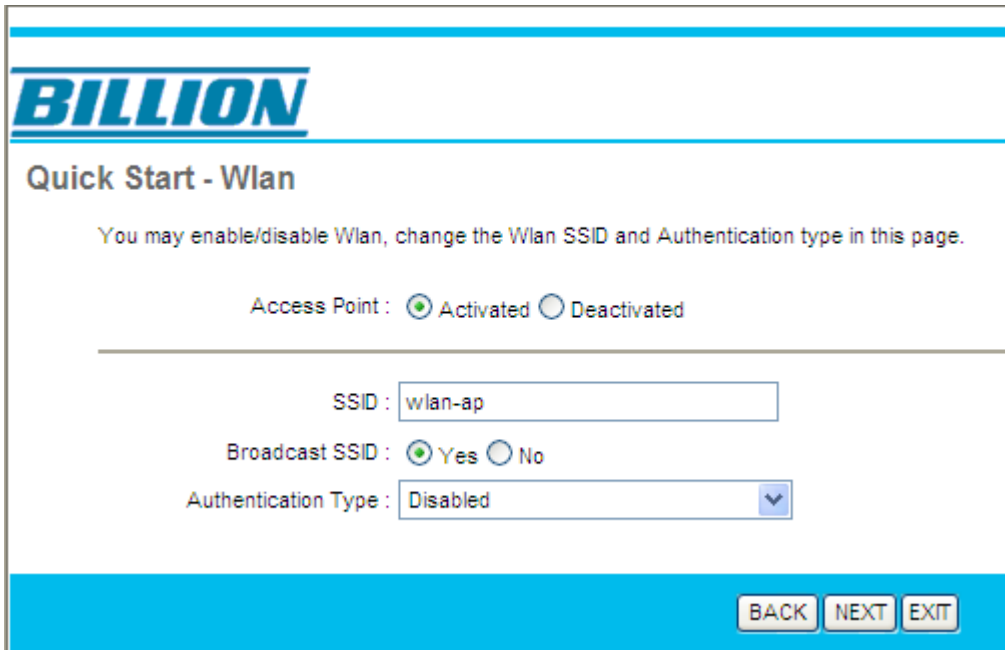
Step 2: Choose your time zone, then click Next.



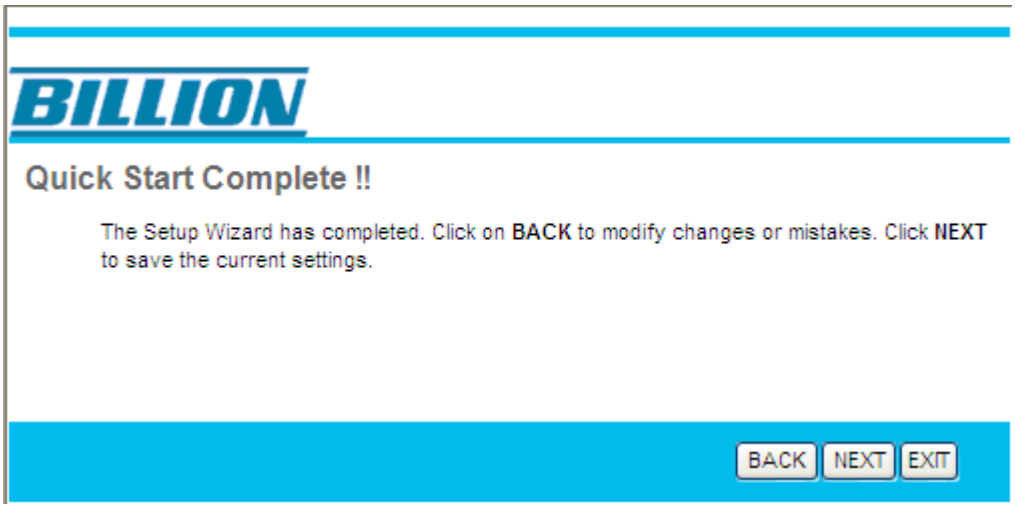
Step 3: Set your internet connection. Choose the appropriate internet connection and enter the necessary information from your ISP.

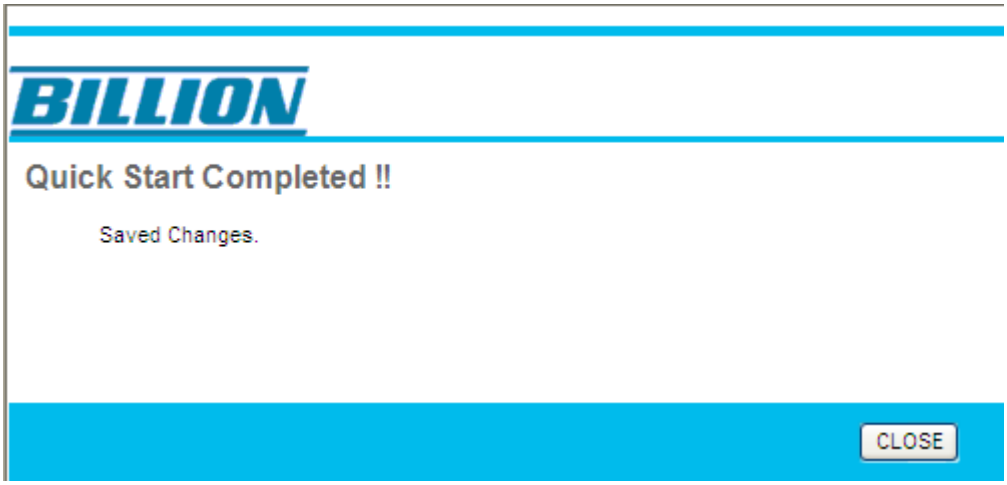


Step 4: Wireless network configuration.



Step 5: Save settings of this ADSL router.





Interface Setup

Click this item to access the following sub-items to configure the router: Internet, LAN and Wireless.

These functions are described in the following sections.

Internet

BILLION

ADSL Modem/Router

Interface | Quick Start | Interface Setup | Advanced Setup | Access Management | Maintenance | Status | Help

Internet | LAN | Wireless

ATM VC

Virtual Circuit : PVC0 [PVCs Summary]

Status : (•) Activated ( ) Deactivated

VPI : 8 (range: 0~255)

VCI : 35 (range: 1~65535)

QoS

ATM QoS : UBR

PCR : 0 cells/second

SCR : 0 cells/second

MBS : 0 cells

Encapsulation

ISP : ( ) Dynamic IP Address

( ) Static IP Address

(•) PPPoA/PPPoE

( ) Bridge Mode

PPPoE/PPPoA

Servicename :

Username : username

Password : ••••••••

Encapsulation : PPPoE LLC

Half Bridge : ( ) Activated (•) Deactivated

Connection Setting

Connection : (•) Always On (Recommended)

( ) Connect On-Demand (Close if idle for 0 minutes)

( ) Connect Manually

TCP MSS Option : TCP MSS(0:default) 0 bytes

IP Address

Get IP Address : ( ) Static (•) Dynamic

Static IP Address : 0.0.0.0

IP Subnet Mask : 0.0.0.0

Gateway : 0.0.0.0

NAT : Enable

Default Route : (•) Yes ( ) No

TCP MTU Option : TCP MTU(0:default) 0 bytes

Dynamic Route : RIP1 Direction : None

Multicast : Disabled

MAC Spoofing : ( ) Enabled (•) Disabled

00:00:00:00:00:00

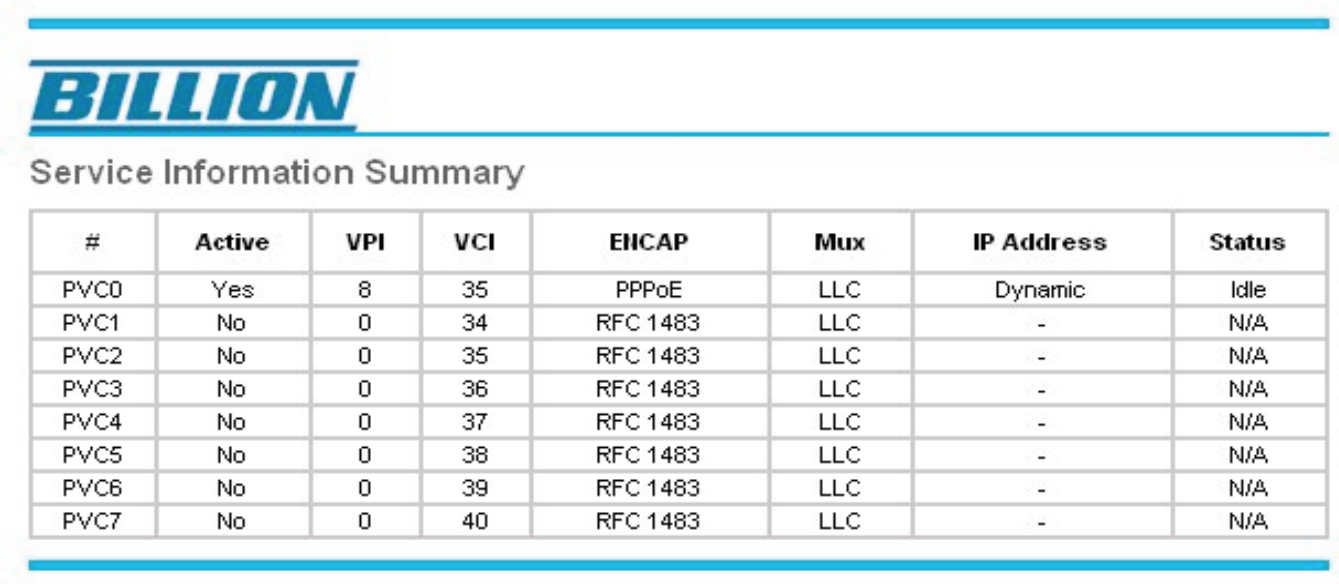
[SAVE]

ATM VC

ATM settings are used to connect to your ISP. Your ISP provides VPI, VCI settings to you. In this Device, you can setup a total of 8 VCs on different encapsulations, if you apply 8 different virtual circuits from your ISP. You need to activate the VC for it to take effect. For PVCs management, you can use ATM QoS to setup each the priority of each PVC traffic line.

Virtual Circuit: VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) defines a virtual circuit.

PVC Summary:



Service Information Summary

#	Active	VPI	VCI	ENCAP	Mux	IP Address	Status
PVC0	Yes	8	35	PPPoE	LLC	Dynamic	Idle
PVC1	No	0	34	RFC 1483	LLC	-	N/A
PVC2	No	0	35	RFC 1483	LLC	-	N/A
PVC3	No	0	36	RFC 1483	LLC	-	N/A
PVC4	No	0	37	RFC 1483	LLC	-	N/A
PVC5	No	0	38	RFC 1483	LLC	-	N/A
PVC6	No	0	39	RFC 1483	LLC	-	N/A
PVC7	No	0	40	RFC 1483	LLC	-	N/A

VPI: The valid range for the VPI is from 0 to 255. Enter the VPI assigned to you. This field may already be configured.

VCI: The valid range for the VCI is from 1 to 65535. Enter the VCI assigned to you. This field may already be configured.

ATM QoS: Select the type of Quality of Service for this Virtual Circuit. The ATM QoS types include CBR (Constant Bit Rate), rtVBR (Real Time Variable Bit Rate), nrtVBR (Non Real Time Variable Bit Rate) and UBR (Unspecified Bit Rate). These types of QoS are all controlled by the parameters specified below, including PCR, SCR and MBS.

Select CBR to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR for applications that are non-time sensitive, such as e-mail. Select VBR for burst traffic applications and those that share bandwidth with other applications.

PCR: Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send the cells.

SCR: The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted.

MBS: Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.

Encapsulation

ISP: Select the encapsulation type your ISP uses from the Encapsulation list. Choices vary depending on what you select in the Mode field.

- **Dynamic IP:** Select this option if your ISP provides you an IP address automatically. This option is typically used for Cable services. Please enter the Dynamic IP information accordingly.

- **Static IP:** Select this option to set static IP information. You will need to enter in the Connetion type, IP address, subnet mask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

- **PPPoE/PPPoA:** Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL services. Select Dynamic PPPoE to obtain an IP address automatically for your PPPoE connection. Select Static PPPoE to use a static IP address for your PPPoE connection. Please enter the information accordingly.

- **Bridge Mode:** Mainly use the MAC address to determine whether to forward data, in this way, the router works like a switch. Select this mode if your ISP uses this mode.

PPPoE / PPPoA

Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL services. Select Dynamic PPPoE to obtain an IP address automatically for your PPPoE connection. Select Static PPPoE to use a static IP address for your PPPoE connection. Please enter the information accordingly.

Service Name: Enter a name for the PPPoE connection.

User Name: Enter the user name exactly as your ISP assigned.

Password: Enter the password associated with the user name above.

Encapsulation: select Bridge in the Mode field, select either PPPoA or RFC 1483. Select Routing in the Mode field, select PPPoA, RFC 1483, ENET ENCAP or PPPoE. Multiplex: Select the method of multiplexing used by your ISP. Choices are VC or LLC.

Half Bridge: The Half Bridge mode can only be used when a single IP address has been assigned by the ISP. It is used when the use of NAT is not desired and there is a single computer attached to the router.

- **Connection:** The schedule rule(s) have priority over your Connection settings.

- **Always on:** Select Always on Connection when you want your connection up all the time.

- **Connect on Demand:** Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.

TCP MSS Option: Enter the TCP Maximum Segment Size (MSS).

Get IP Address: Choose Static or Dynamic.

Static IP Address: Enter the IP address of ADSL Router in dotted decimal notation, for example, xx.xx.xx.xx.

IP Subnet Mask: The default is 0.0.0.0. User can change it to other such as 255.255.255.0.Type the subnet mask assigned to you by your ISP (if given).

Gateway: You must specify a gateway IP address (supplied by your ISP) when you use 1483

Bridged IP in the Encapsulation field in the previous screen.

NAT: Select this option to Activate/Deactivated the NAT (Network Address Translation) function for this VC. The NAT function can be activated or deactivated per PVC basis.**Default Route:** if enable this function, the current PVC will be the default gateway to internet from this device.

TCP MTU Option: Enter the TCP maximum transmission unit (MTU).

Dynamic Route:

- **RIP Version:** (Routing Information protocol) Select this option to specify the RIP version, including RIP-1, RIP2-M and RIP2-B. RIP2-M and RIP2-B are both sent in RIP-2 format; the difference is that RIP2-M using Multicast and RIP2-B using Broadcast format.

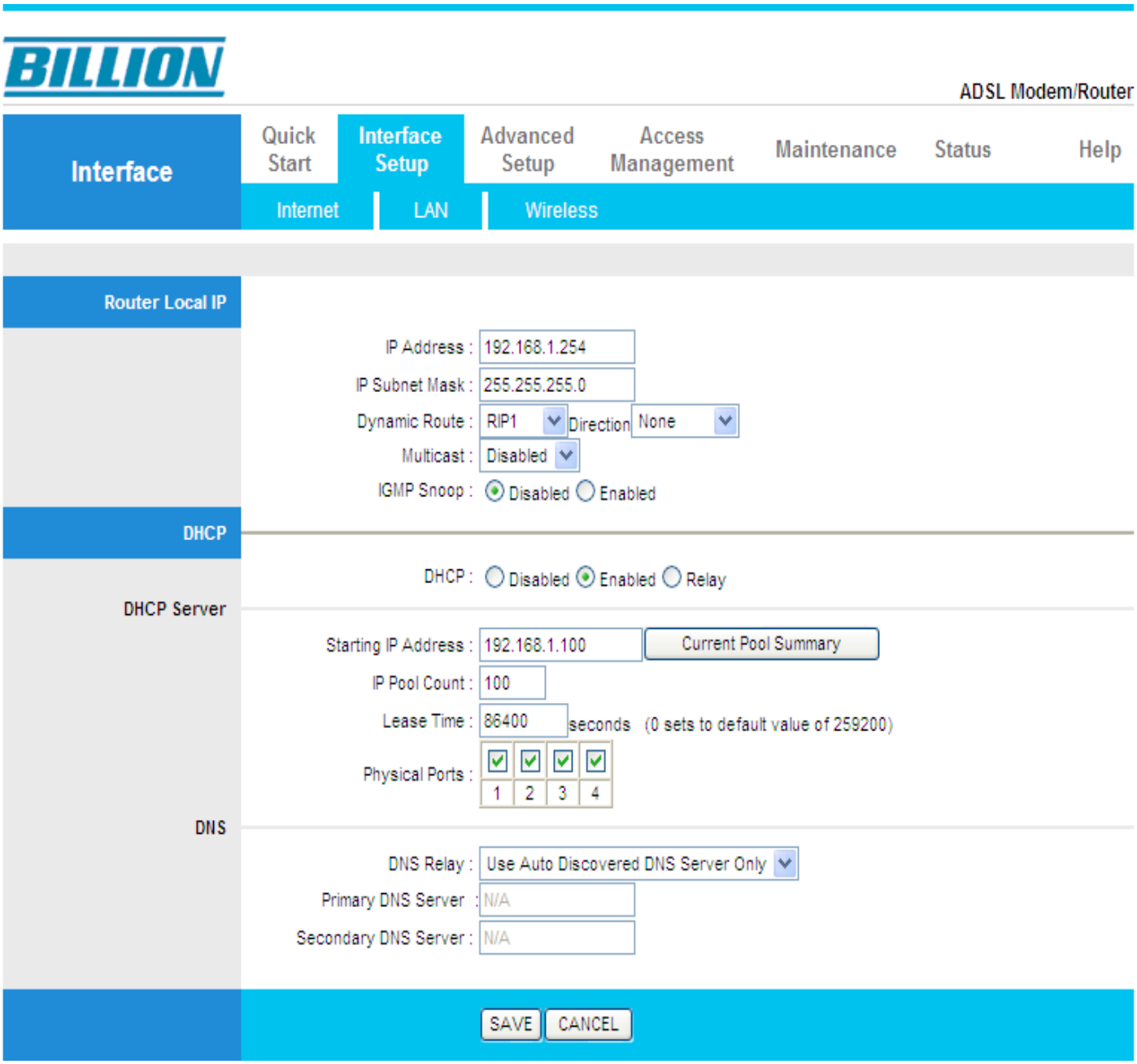
- **RIP Direction:** Select this option to specify the RIP direction. None is for disabling the RIP function. Both means the ADSL Router will periodically send routing information and accept routing information then incorporate into routing table. IN only means the ADSL router will only accept but will not send RIP packet. OUT only means the ADSL router will only send but will not accept RIP packet.

Multicast: IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. BiPAC 5200G *RC* Series router supports IGMP-v1, IGMP-v2 and IGMP-v3. Select Disabled to disable this function.

MAC Spoofing: You can either choose to enable or disable MAC spoofing feature. Some service providers may require the configuration of this feature. When this feature is enabled, enter the MAC address assigned by your service providers in the blank provided.

LAN

A Local Area Network (LAN) is a shared communication system to which many computers are attached and is limited to the immediate area, usually the same building or floor of a building.



Router Local IP

IP Address: Enter the IP address of ADSL Router in dotted decimal notation, for example, 192.168.1.254 (factory default).

IP Subnet Mask: The default is 255.255.255.0. User can change it to other such as 255.255.255.128.

Dynamic Route: Select the RIP version from RIP-1, RIP2-B and RIP2-M.

RIP Direction: Select the RIP direction from None, Both, In Only and Out Only.

Multicast: IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish

membership in a Multicast group - it is not used to carry user data. BiPAC 5200G *RC* Series router supports IGMP-v1, IGMP-v2 and IGMP-v3. Select Disabled to disable the function.

IGMP Snoop: IGMP helps to reduces the network traffic.Choose Disable or Enable IGMP Snoop function.

DHCP

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server.

DHCP: If set to Enable, your router can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.

If set to disabled, the DHCP server will be disabled.

If set to Relay, your router acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.

When DHCP is used, the following items need to be set.

Starting IP Address: This field specifies the first of the contiguous addresses in the IP address pool.

IP Pool Count: This field specifies the size or count of the IP address pool.

Lease Time: The current lease time of client.

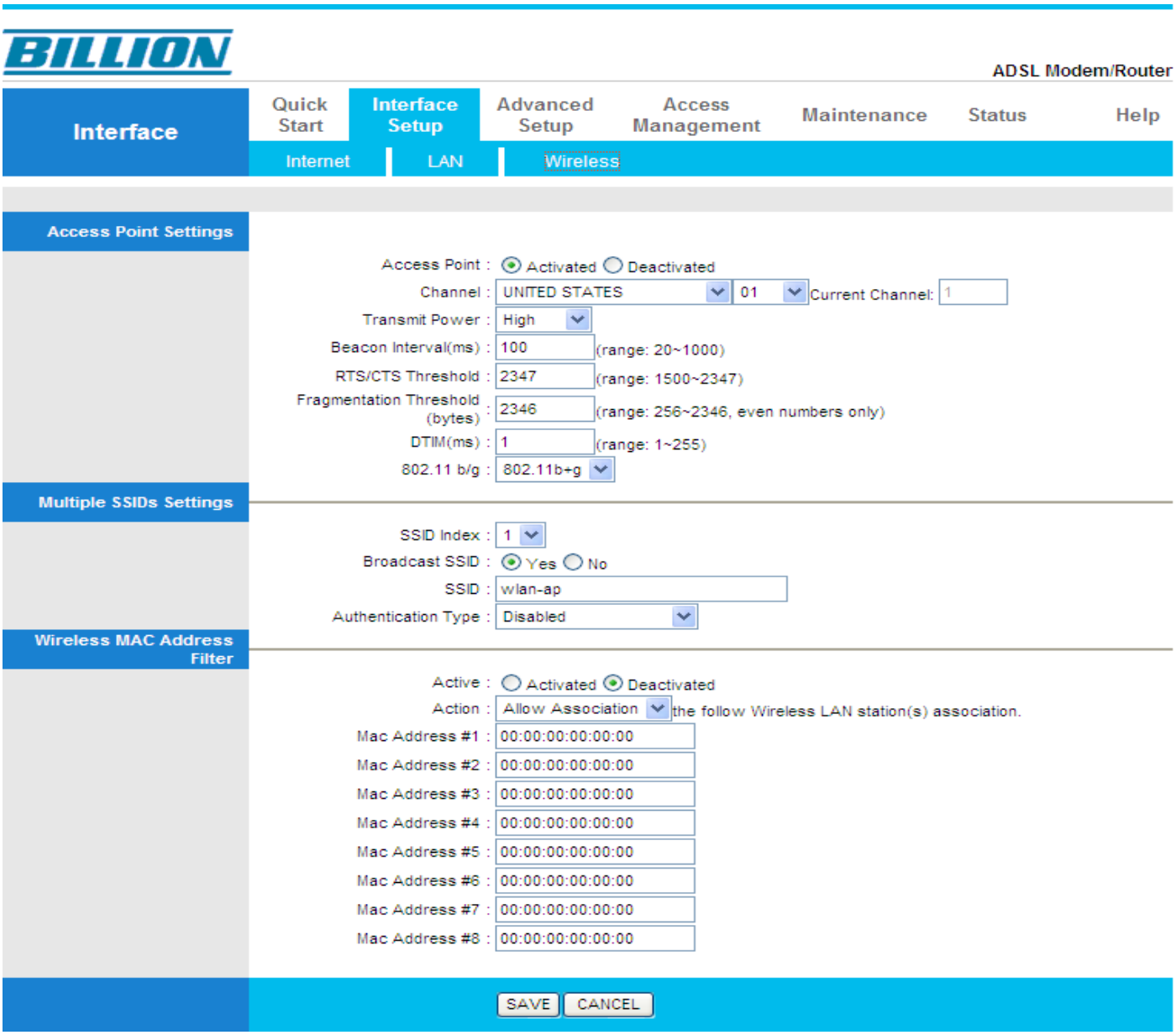
DNS Relay: Use the Local computer as a DNS Server, but without any resolution, it pass the work to another DNS Server which the DNS Relay points to. The specified Server do the resolution work and pass the result to the Local server and then the local server pass the received result to the client. Select from the drop-down menu to specify the another server which does the resolution work.

Primary DNS Server: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Secondary DNS Server: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Wireless

This section introduces the wireless LAN and some basic configurations. Wireless LANs can be as simple as two computers with wireless LAN cards communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to the wired LAN.



Access Point Setting

Access Point: Default setting is set to Activated. If you do not have any wireless, both 802.11g and 802.11b, device in your network, select Deactived.

Channel ID: The range of radio frequencies used by IEEE 802.11b/g wireless devices is called a channel. Select a channel from the drop-down list box.

Transmit Power: User can customize the transmit power to either high, medium or low.

Beacon interval: The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network.

RTS/CTS Threshold: The RTS (Request To Send) threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake.

Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake Enter a value between 1500 and 2347.

Fragmentation Threshold: The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2346.

DTIM: This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM).

802.11b/g: The default setting is 802.11b+g (Mixed mode). If you do not know or have both 11g and 11b devices in your network, then keep the default in mixed mode. From the drop-down manual, you can select 802.11g if you have only 11g card. If you have only 11b card, then select 802.11b.

Multiple SSIDs Setting

SSID Index: Default SSID index is “1”.

Broadcast SSID: Select Yes to make the SSID visible so a station can obtain the SSID through passive scanning. Select No to hide the SSID in so a station cannot obtain the SSID through passive scanning.

SSID: The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change the default wlan-ap to a unique ID name to the AP which is already built-in to the router’s wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.

Authentication Type: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP & WPA. If you require high security for transmissions, there are four alternatives to select from: 64-bit WEP, 128-bit WEP, WPA-PSK and WPA2-PSK. WEP 128 will offer increased security over WEP 64.

You can disable or enable WPA or WEP for protecting wireless network. The default type of wireless is disabled and to allow all wireless computers to communicate with the access points without any data encryption.

Wireless MAC Address Filter

The MAC filter screen allows you to configure the router to give exclusive access up to 8 devices (Allow Association) or exclude up to 8 devices from accessing the router (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:AA:BB:00:00:02. You need to know the MAC address of the devices to configure this screen.

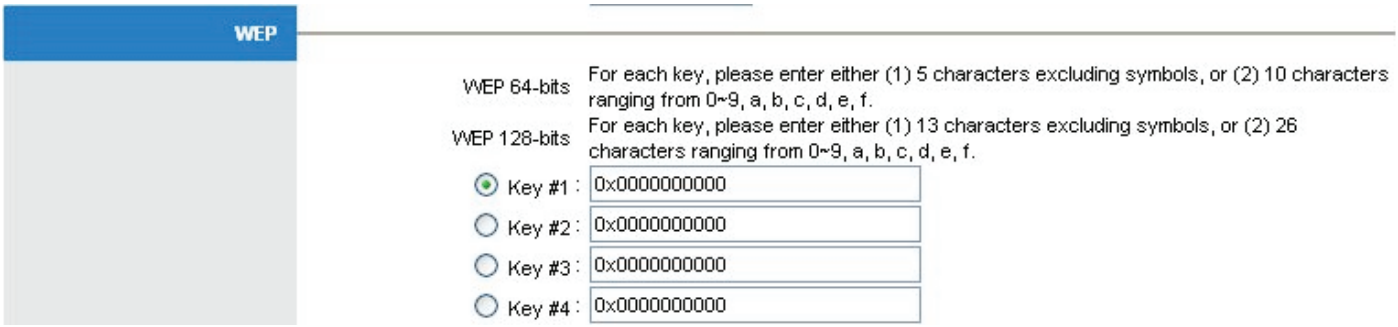
Active: Select Actived to enable MAC address filtering.

Action: Define the filter action for the list of MAC addresses in the MAC address filter table.

Select Deny Association to block access to the router, MAC addresses not listed will be allowed to access the router. Select Allow Association to permit access to the router, MAC addresses not listed will be denied access to the router.

MAC Address: Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the router in these address fields.

WEP



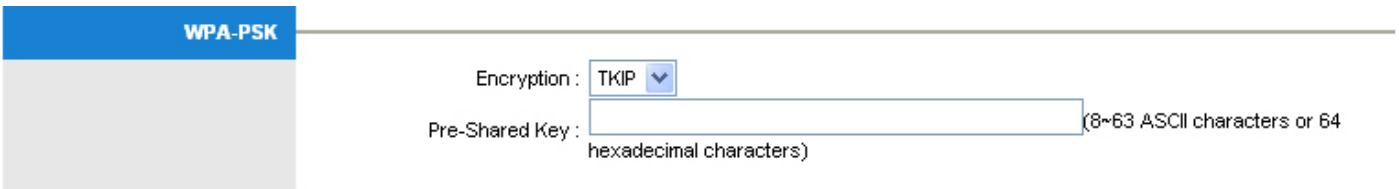
Key 1 to Key 4: Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys to your selection. The input format is in HEX style, 10 and 26 HEX codes are required for 64-bit WEP and 128-bit WEP respectively.

If you choose WEP 64-bits, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").

If you choose WEP 128-bits, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").

You can configure all four keys, but only one key can be activated at any one time. The default key is key 1.

WPA-PSK & WPA2-PSK



Encryption: TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption System) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

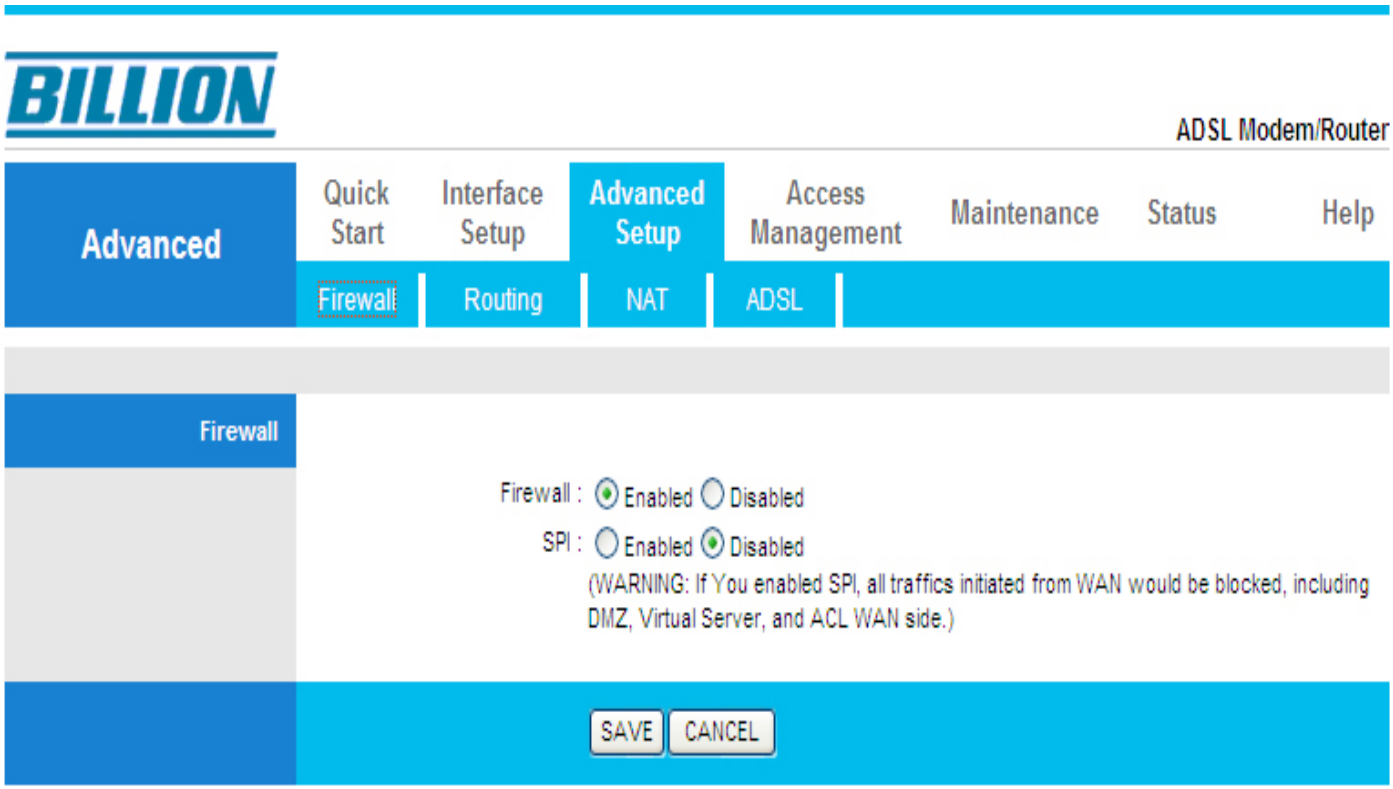
Pre-Shared key: The key for network authentication. The input format should be 8-63 ASKII

characters or 64 hexadecimal characters.

Advanced Setup

Firewall

Your router includes a firewall for controlling Internet access from your LAN that helps to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet.



Firewall: to automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

Enabled: As set in default setting, it activates your firewall function.

Disabled: It disables the firewall function.

SPI: If you enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

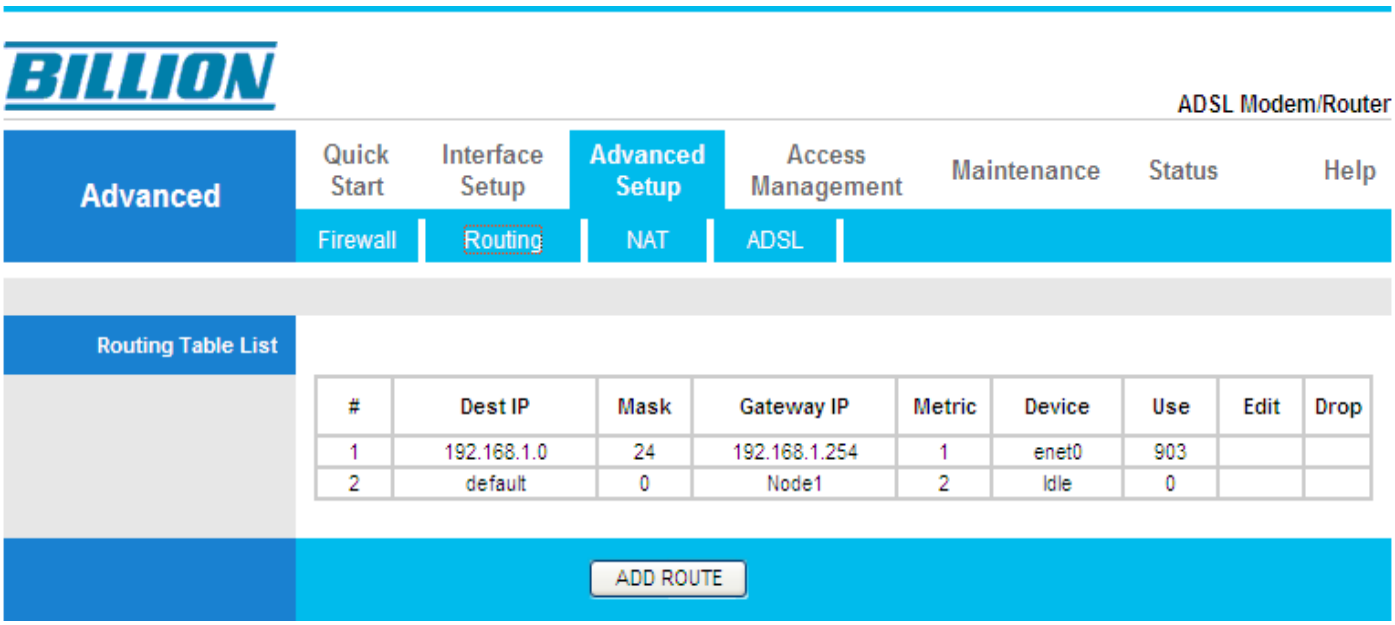
Enabled: As set in default setting, it activates your SPI function.

Disabled: It disables the SPI function.

Press **SAVE** to apply your settings.

Routing

If you have another router with a LAN-to-LAN connection, you may create a static routing on the router that is the gateway to Internet.



#	Dest IP	Mask	Gateway IP	Metric	Device	Use	Edit	Drop
1	192.168.1.0	24	192.168.1.254	1	enet0	903		
2	default	0	Node1	2	Idle	0		

#: Item number

Dest IP: IP address of the destination network

Mask: The destination mask address.

Gateway IP: IP address of the gateway or existing interface that this route uses.

Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

Device: Media/channel selected to append the route.

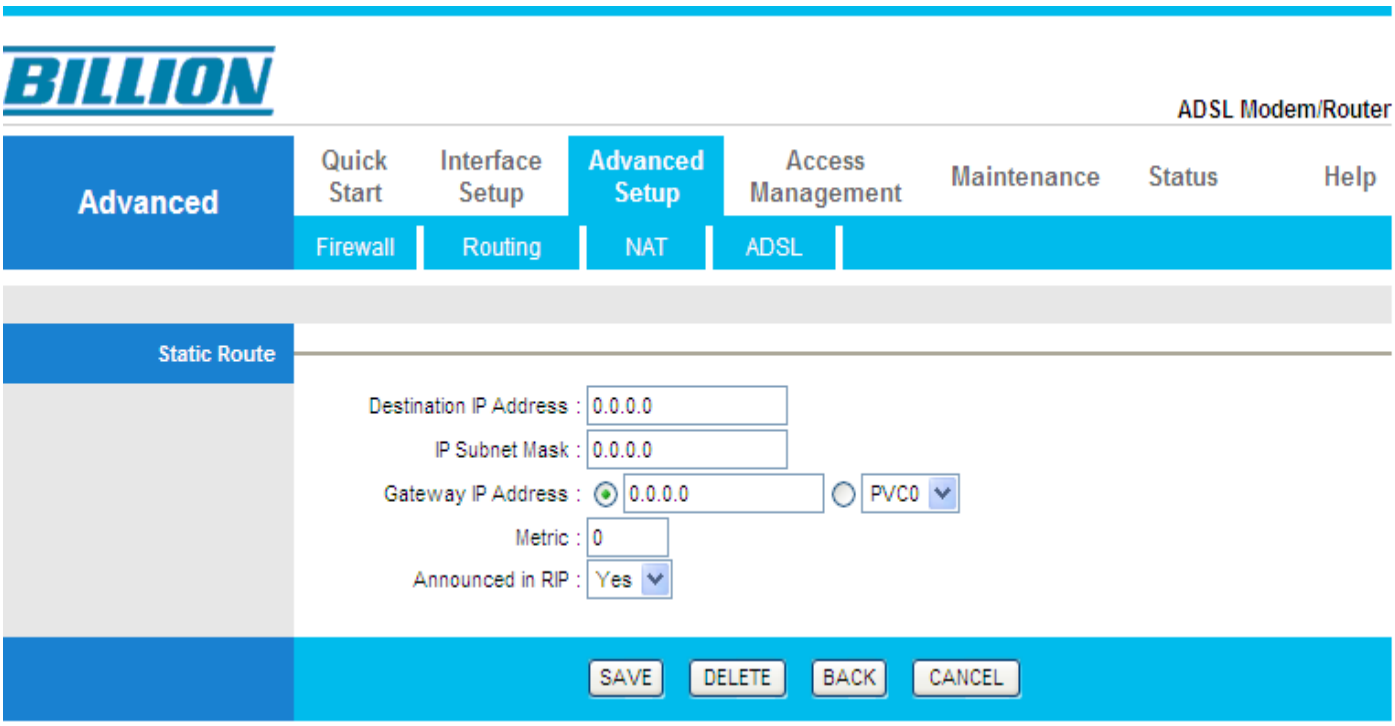
Use: the statistics of the packets received and transmitted.

Edit: Edit the route; this icon is not shown for system default route.

Drop: Drop the route; this icon is not shown for system default route.

Add Route

To add a new route, press the Add Route button. Then fill in all the parameters needed for the route. When done, press the Save button.



Destination IP Address: This is the destination subnet IP address.

IP Subnet Mask: A subnet mask allows IP networks to be subdivided for security and performance purposes.

Gateway IP Address: This is the gateway IP address to which packets are to be forwarded.

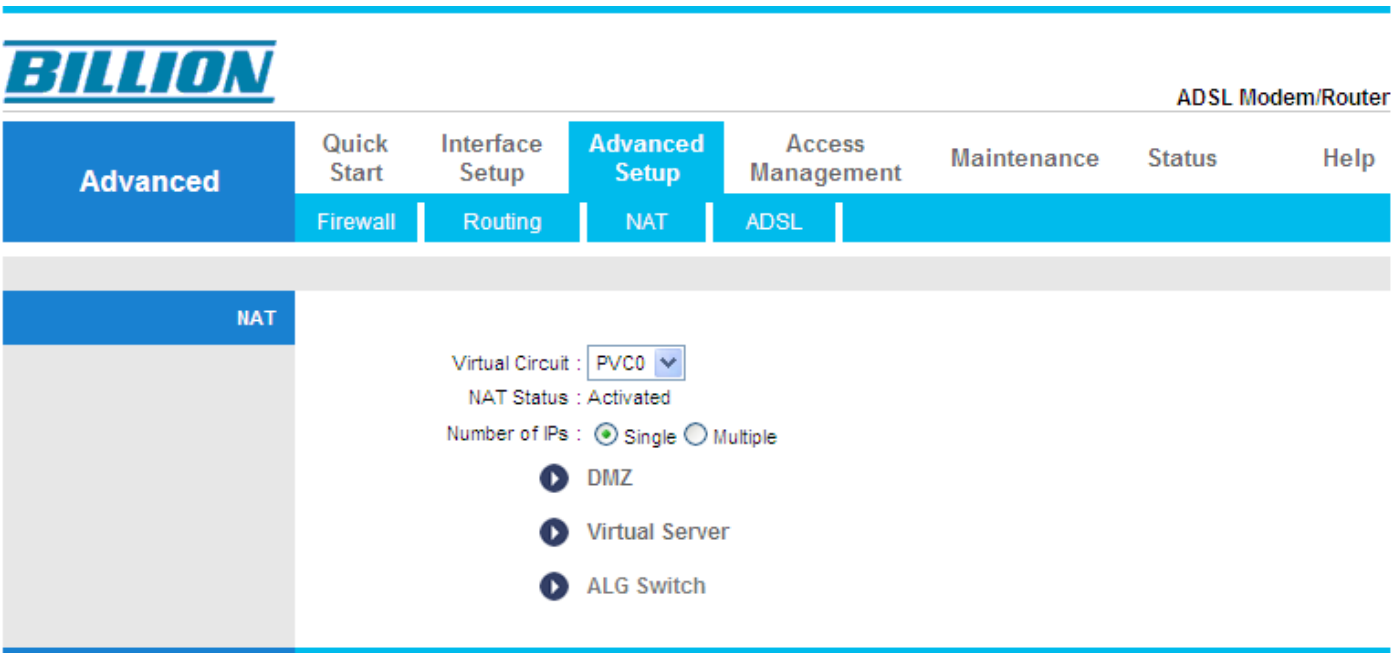
Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

Announced in RIP: This parameter determines if the Prestige will include the route to the remote node in its RIP broadcasts. Set “No”, it is kept private and is not included in RIP broadcasts. Set “Yes”, the remote node will be propagated to other hosts through RIP broadcasts.

Press **SAVE** to apply your settings and the item you added will be listed in the **Routing Table List**.

NAT

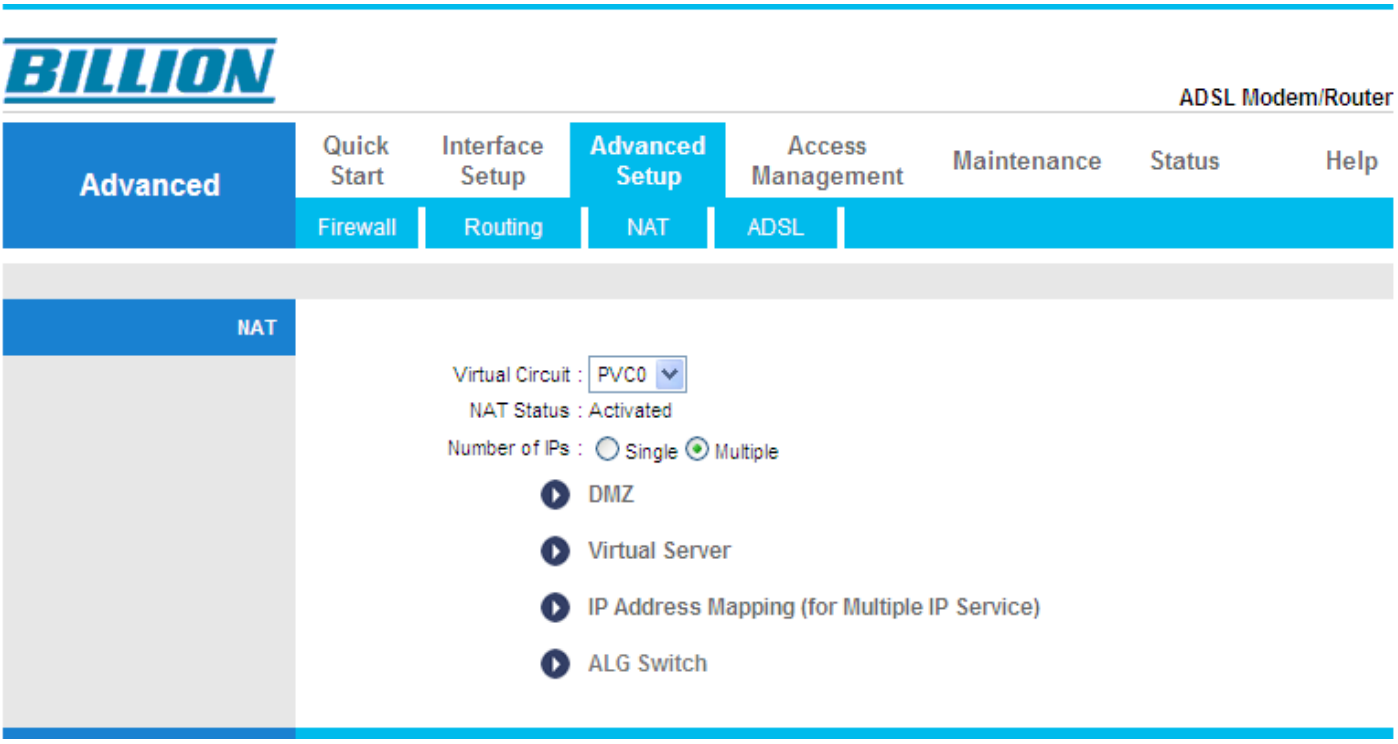
The NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. The default setting is Dynamic NAT. It provides dynamic Network Address Translation capability between LAN and multiple WAN connections, and the LAN traffic is routed to appropriate WAN connections based on the destination IP addresses and Route Table. This eliminates the need for the static NAT session configuration between multiple LAN clients and multiple WAN connections.



Virtual Circuit: VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) defines a virtual circuit. There are eight groups of PVC that can be defined and used.

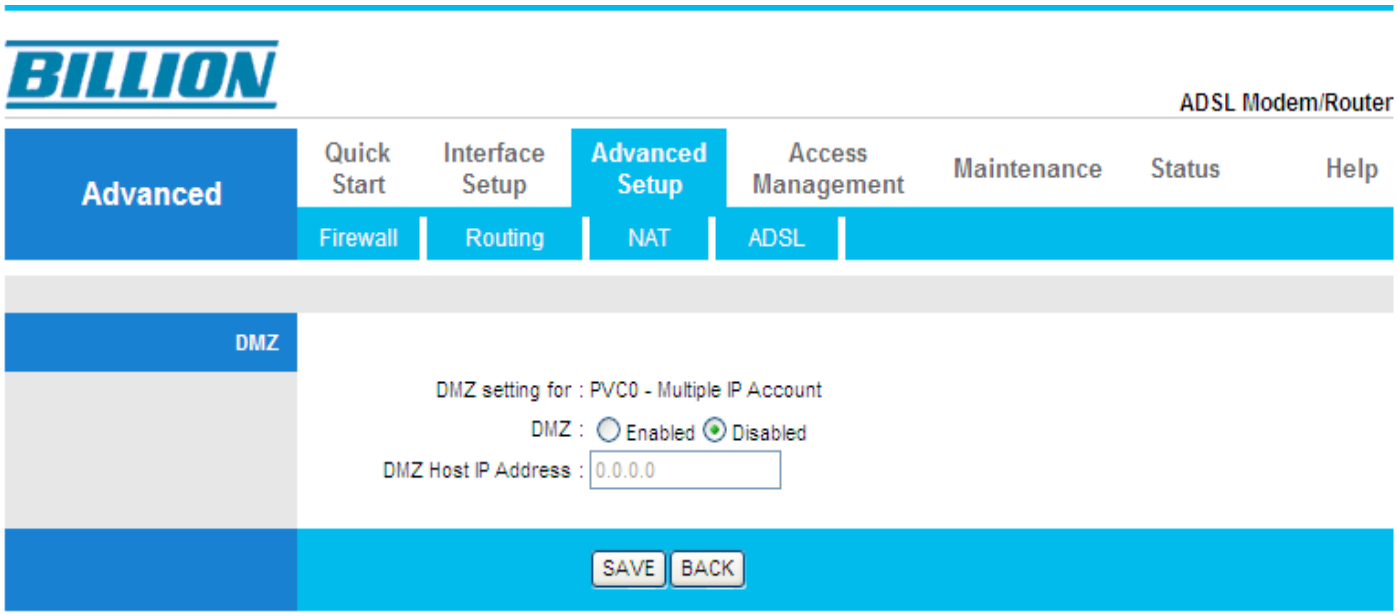
NAT Status: Show the NAT status, Activated or Deactivated.

Number of IPs: User can select Single or Multiple. Select Multiple to trigger IP Address Mapping.



DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets that do not use a port number which is already used by any other Virtual Server entries will first be checked by the Firewall and NAT algorithms before it is passed to the DMZ host.



DMZ setting for: indicate the related LAN PC and PVC ports which allow outside network to connect in and communicate.

DMZ:

Disabled: As set in default setting, it disables the DMZ function.

Enabled: It activates your DMZ function.

DMZ Host IP Address: Give a static IP address to the DMZ Host when Enabled radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

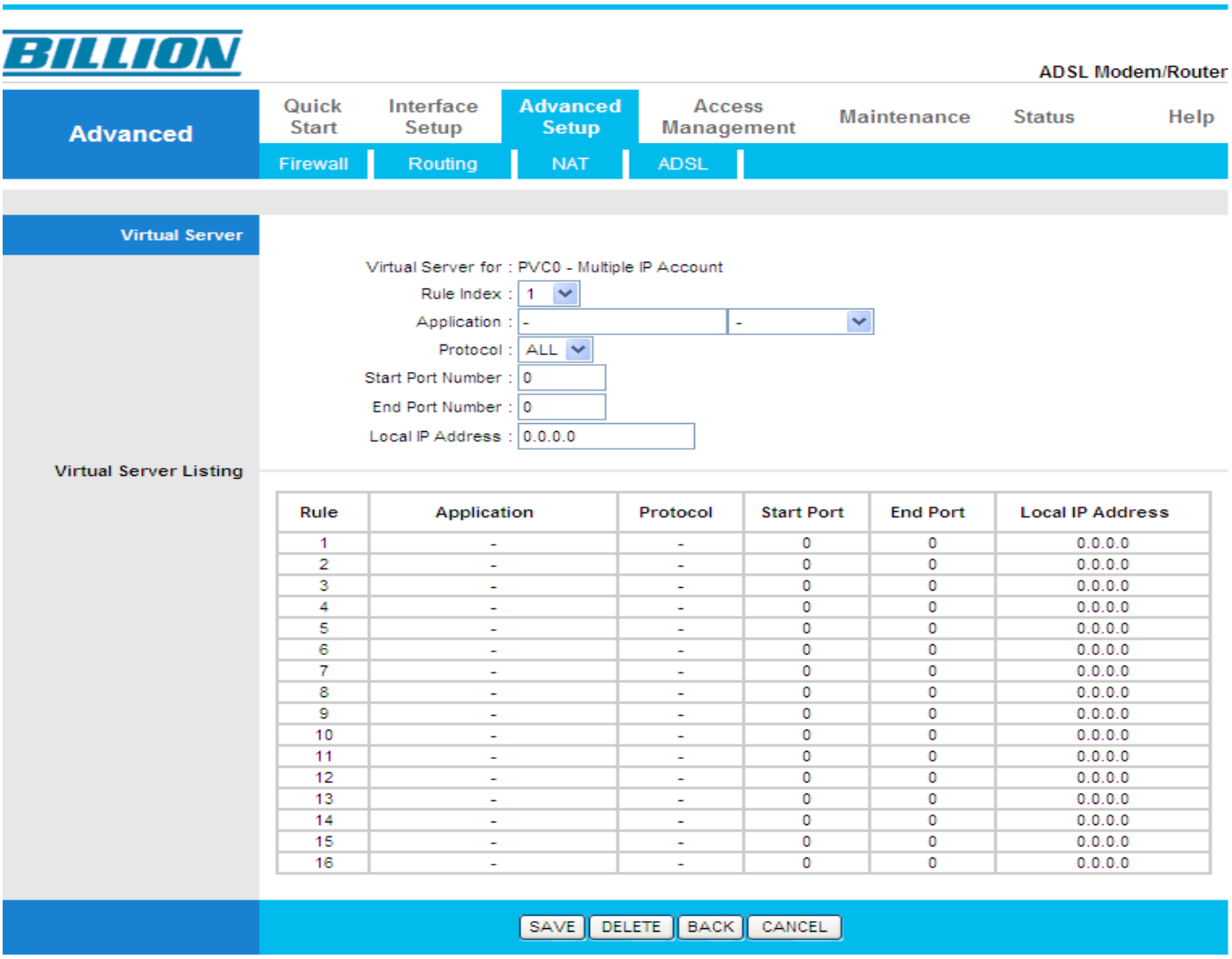
Select the **SAVE** button to apply your changes.

Virtual Server

In TCP/IP and UDP networks, a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts to the PC on your network using specific ports. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by yourPCs. Please see the WAN configuration section of this manual for more information on NAT.The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to the local servers on the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.



Rule Index: Choose the rule number.

Application: Choose the predefined rule from Application drop-down menu or enter a custom name.

Protocol: Choose the Protocol Type, ALL, TCP or UDP.

Start Port Number: Enter a port number as the beginning number of the range which you want to give to devices to access in this field.

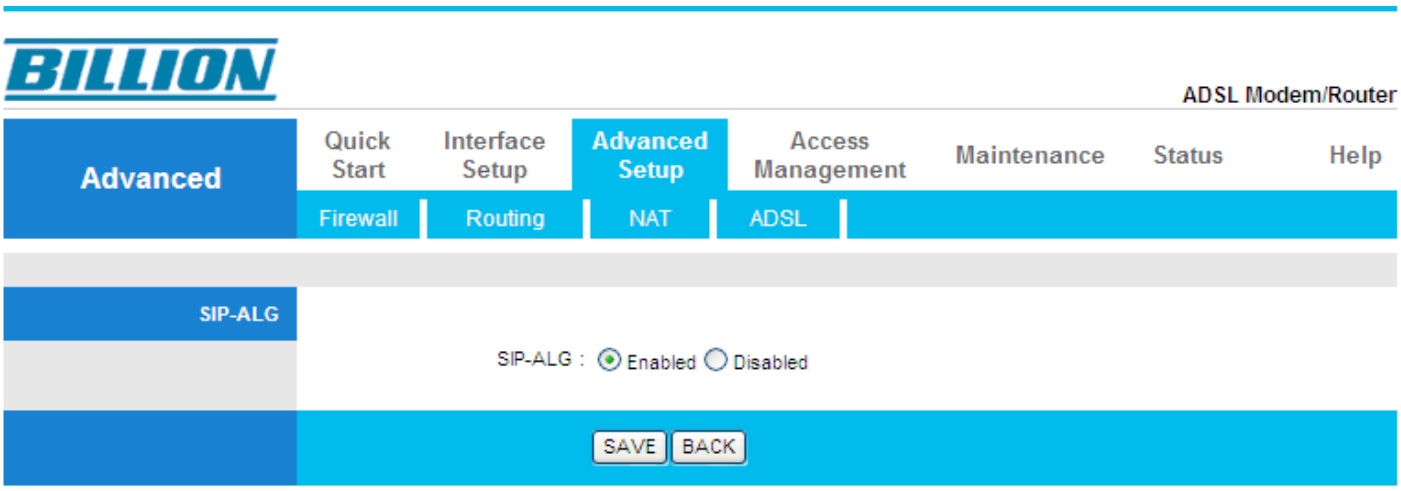
End Port Number: Enter a port number as the ending number of the range which you want to give to devices to access in this field.**Local IP Address:** Enter your server IP address in this field.

Local IP Address: Enter your server IP address in this field.

Press **SAVE** to confirm your settings, and the item you added will be listed in the **Virtual Server Listing** table below. Select the rule index of the item you want to delete from the **Rule Index** drop-down menu, press **DELETE** and you will delete it.

ALG Switch

In the context of computer networking, an application-level gateway (also known as ALG or application layer gateway) consists of a security component that augments a firewall or NAT employed in a computer network. It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, BitTorrent, SIP, RTSP, file transfer in IM applications etc. In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.



SIP-ALG: select Enabled to activate SIP ALG feature or Disabled to disable this feature.

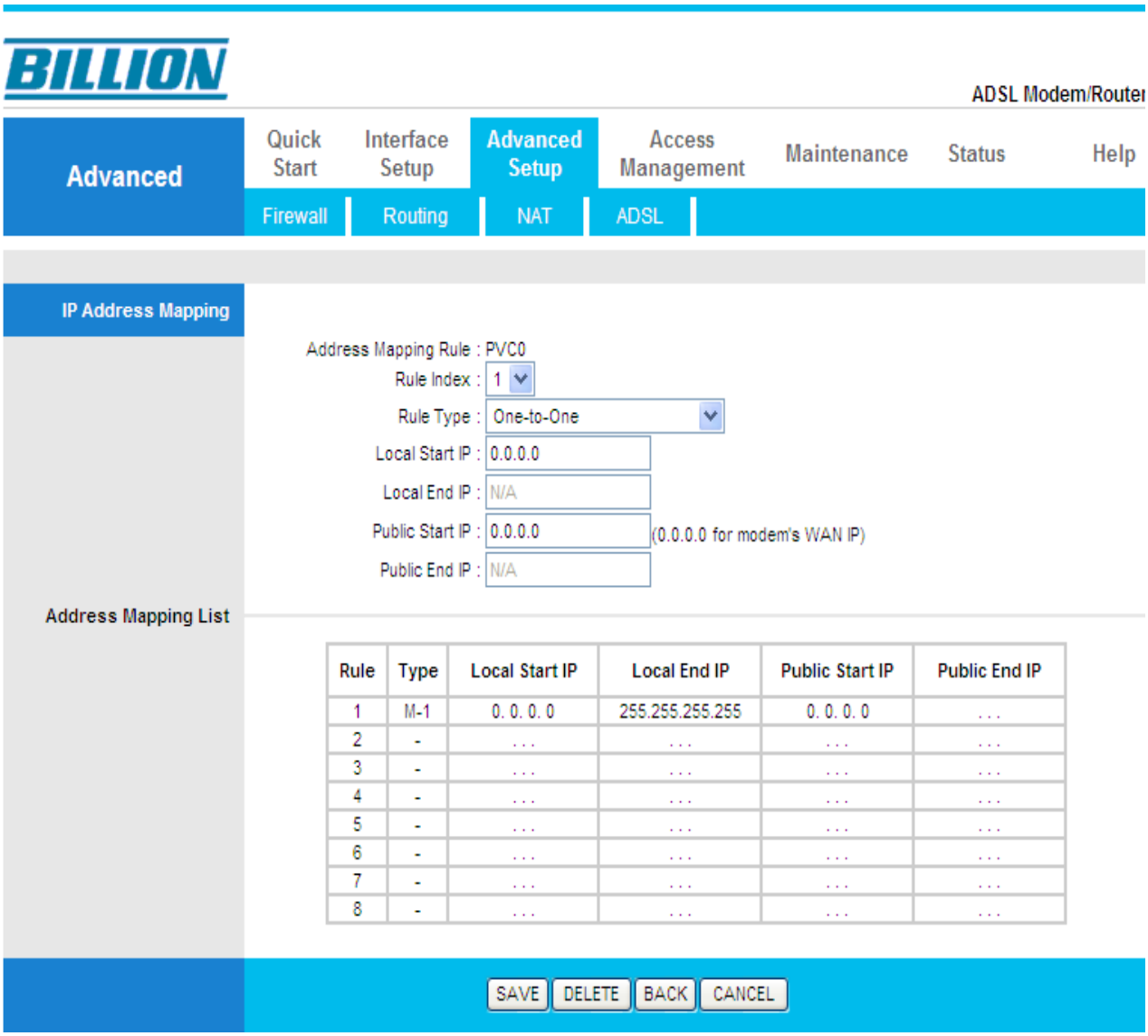
The Session Initiation Protocol (SIP) is an IETF-defined signaling protocol, widely used for controlling multimedia communication sessions such voice and video calls over Internet protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. It is a text-based Application Layer protocol.

But as many use NAT to communicate with the public networks, and the IP address and port combination in SIP packets are needed for addressing, we must come up with an effective way to deal with SIP NAT traversal. SIP ALG is an easy solution with which you are only required to enable SIP ALG on NAT application in this router to easily experience the smooth SIP connection between private networks and public networks or even in two private networks with your VoIP devices.

Press **SAVE** button to apply your settings.

IP Address Mapping

Address Mapping Rule: Shows the PVC where the rule will be applied to.



Rule Index: Choose the rule number.

Rule Type:

- One-to-one: This is the mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.
- Many-to-One: This is the mode maps multiple local IP addresses to one global IP address. This is equivalent to Many to One (i.e., PAT, port address translation).
- Many-to-Many Overload: This mode maps multiple local IP addresses to shared global IP addresses.
- Many-to-Many No Overload: This mode maps each local IP address to an unique global IP addresses.
- Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Local Start IP: This is the starting range for Inside Local IP Address (ILA). Local IP addresses are

N/A for Server port mapping.

Local End IP: This is the end range for Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is N/A for One-to-one and Server mapping types.

Public Start IP: This is the start range for Inside Public IP Address. Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.

Public End IP: This is the end range for Inside Public IP Address. This field is N/A for One-to-one, Many-to-One and Server mapping types.

Press **SAVE** to confirm your settings, and the corresponding settings will be listed in the **Address Mapping List** table.

Select the rule index of the item you want to delete from the **Rule Index** drop-down menu, press **DELETE** and you will delete it.

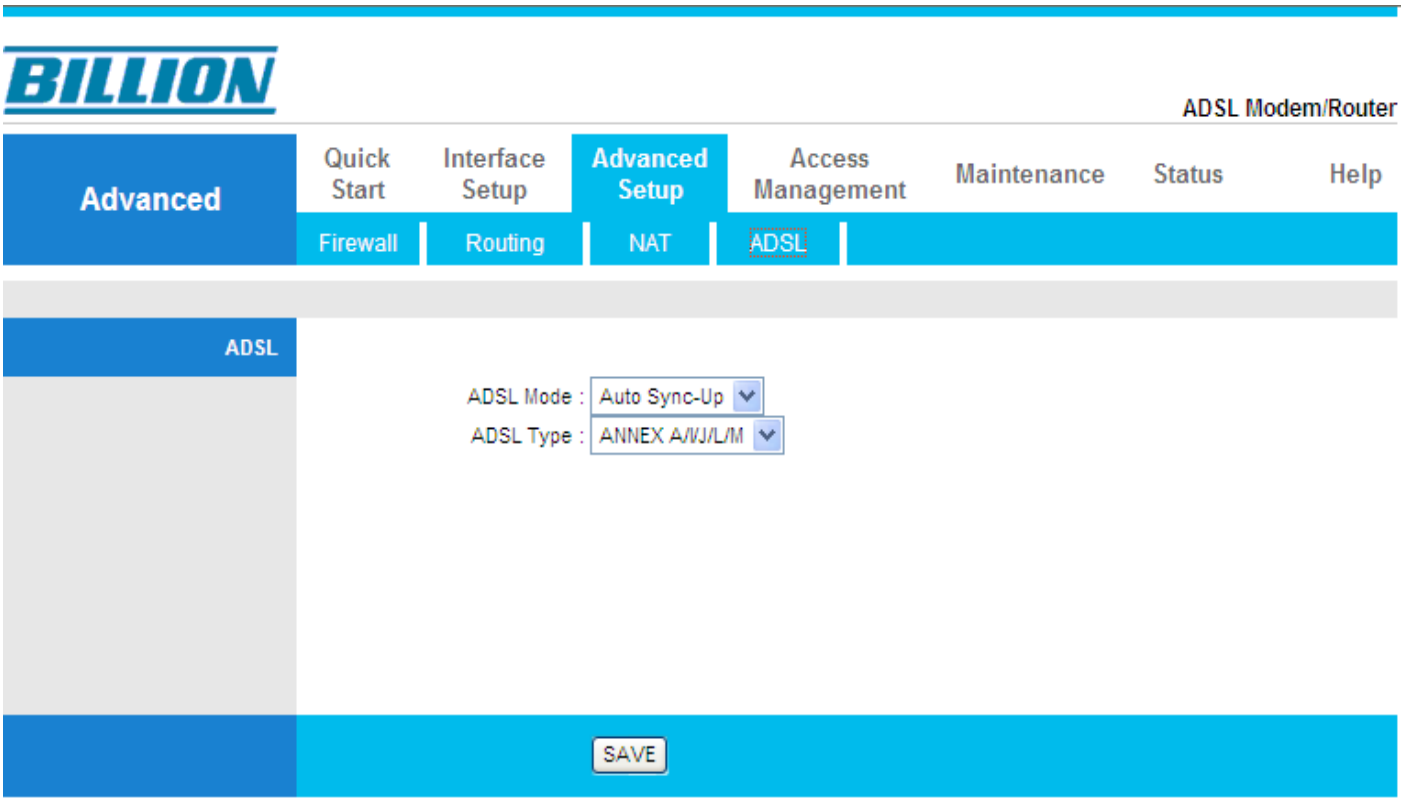
NOTE:

Using Port Forwarding does have implications, as outside users will be able to connect to the PCs on your network. For this reason, you are adviced to use specific Virtual Server entries just for the port your application requires instead of using DMZ. Doing so will result in all connections from WAN to attempt to access the public IP your DMZ specifies.

Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

ADSL



ADSL Mode: The default setting is Auto Sync-UP. This mode will automatically detect your ADSL, ADSL2+, ADSL2, G.dmt, G.lite, and T1.413. But in some area, multimode cannot detect the ADSL line code well. If it is the case, please adjust the ADSL line code to G.dmt or T1.413 first. If it still fails, please try the other values such as ALCTL, ADI, etc.

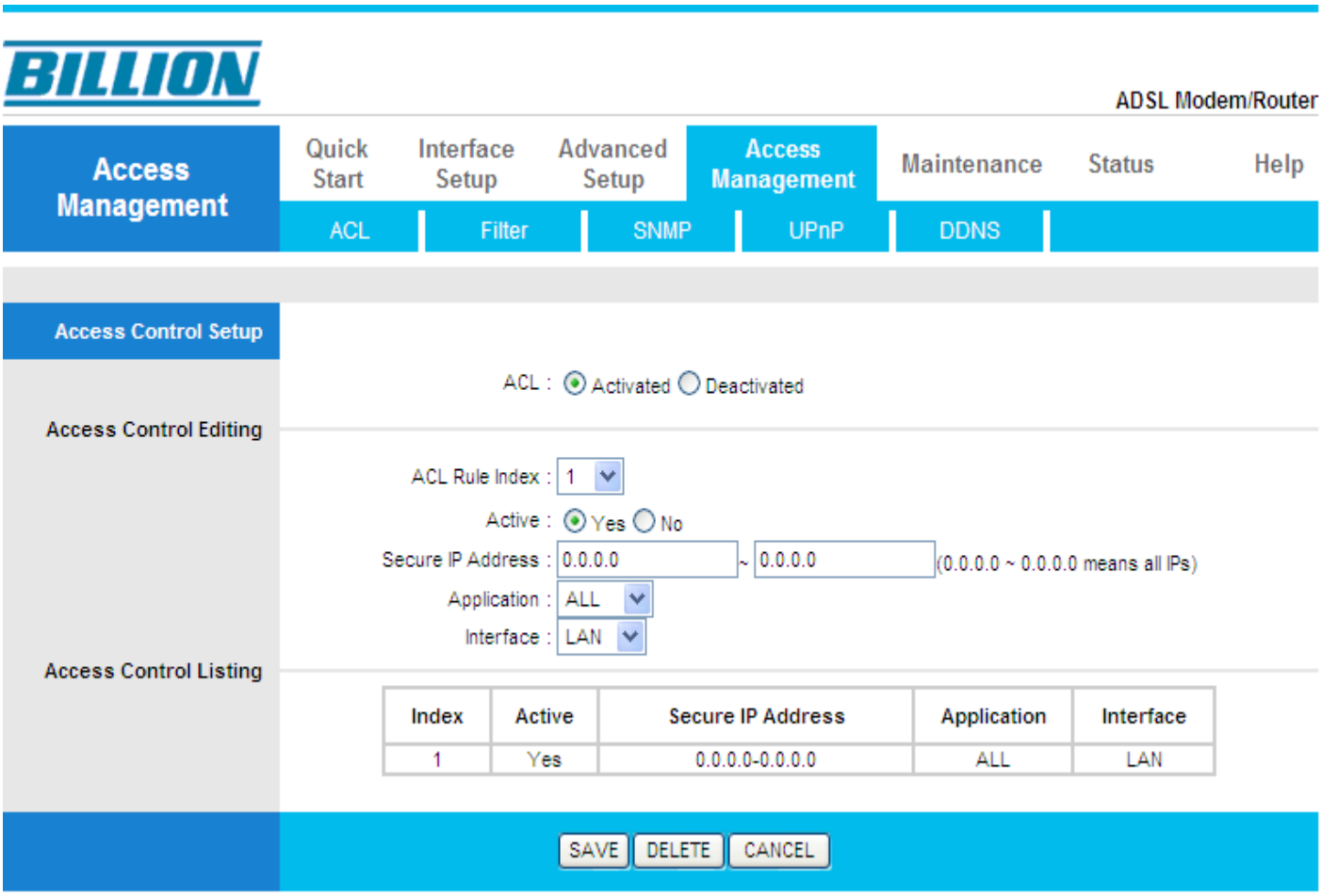
ADSL Type: There are five modes ”Annex A”, ”Annex I”, “Annex A/L”, ”Annex M” and “Annex A/I/J/L/M” that user can select for this connection.

Press **SAVE** to apply your settings.

Access Management

ACL

Access Control Listing allows you to determine which services/protocols can access BiPAC 5200G *RC* Series router interface and from which computers.



ACL: Select whether to activate to configure this ACL function. If you select Deactivated, then the following is not available.

ACL Rule Index: This is item number.

Active: Select Yes to active the ACL function of this rule or No to disable ACL function of this rule.

Secure IP Address: The default 0.0.0.0 allows any client to use this service to remotely manage the your router. Type an IP address to restrict access to a client with a matching IP address.

Application: Choose a service that you may use to remotely manage the router.

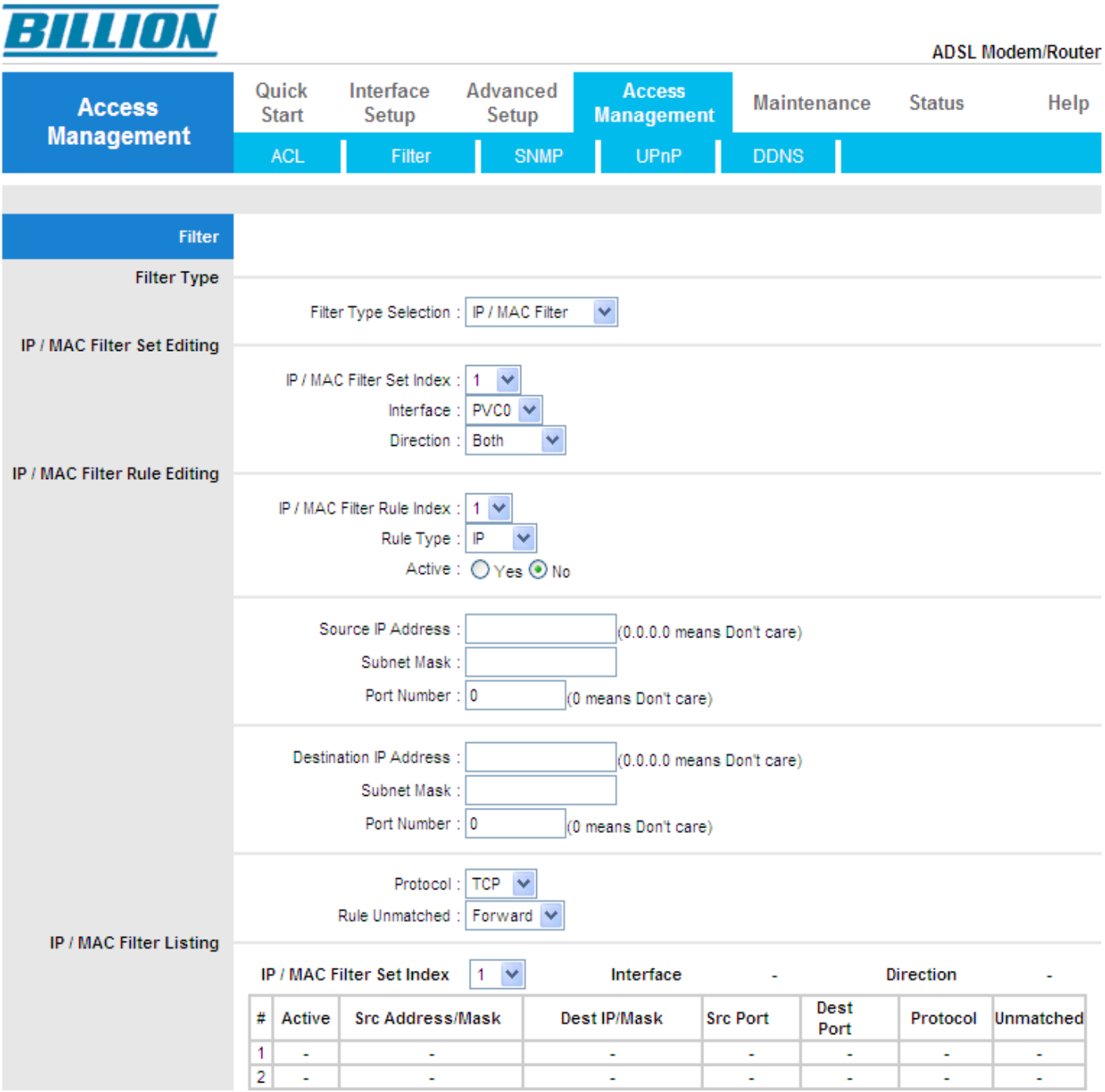
Interface: Select the access interface. Choices are LAN, WAN and Both.

Press **SAVE** to confirm your settings, and the corresponding settings will be listed in the **Address Control Listing** table.

Select the rule index of the item you want to delete from the **ACL Rule Index** drop-down menu, press **delete** and you will delete it.

Filter

You can Filter the packages by IP port, MAC and Application.



Filter Type

Filter Type Selection: There are three types ”IP/MAC Filter”, ”Application Filter”, and “URL Filter” that user can select for this connection.

IP / MAC Filter Set Editing

IP/MAC filter Set Index: This is item number.

Interface: Select which channel (PVC) to configure.

Direction: Select the access to the Internet (“Outgoing”) or from the Internet (“Incoming”) or Both.

IP / MAC Filter Rule Editing

IP/MAC Filter Rule Index: This is item number.

Rule Type: Choose “IP” or “MAC” rules

Active: Select Yes from the drop down list box to enable IP filter rule.

Source IP Address: The source IP address or range of packets to be monitored.

Subnet Mask: It is the source IP addresses based on the above subnet IP source.

Source Port Number: This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range 0 ~ 65535. It is recommended that this option be configured by an advanced user.

Destination IP Address: This is the destination subnet IP address.

Subnet Mask: It is the destination IP addresses based on the above subnet IP destination.

Destination Port Number: This is the Port or Port Ranges that defines the application.

Protocol: It is the packet protocol type used by the application, select either TCP or UDP or ICMP

Rule Unmatched: Select the action for the traffic that does not match the current rule; Forward to leave it pass through, and NEXT to check it by the next rule.

IP / MAC Filter Listing

#: Item number.

Active: Whether the connection is currently active.

Src Address/Mask: The source IP address or range of packets to be monitored.

Dest IP/Mask: This is the destination subnet IP address.

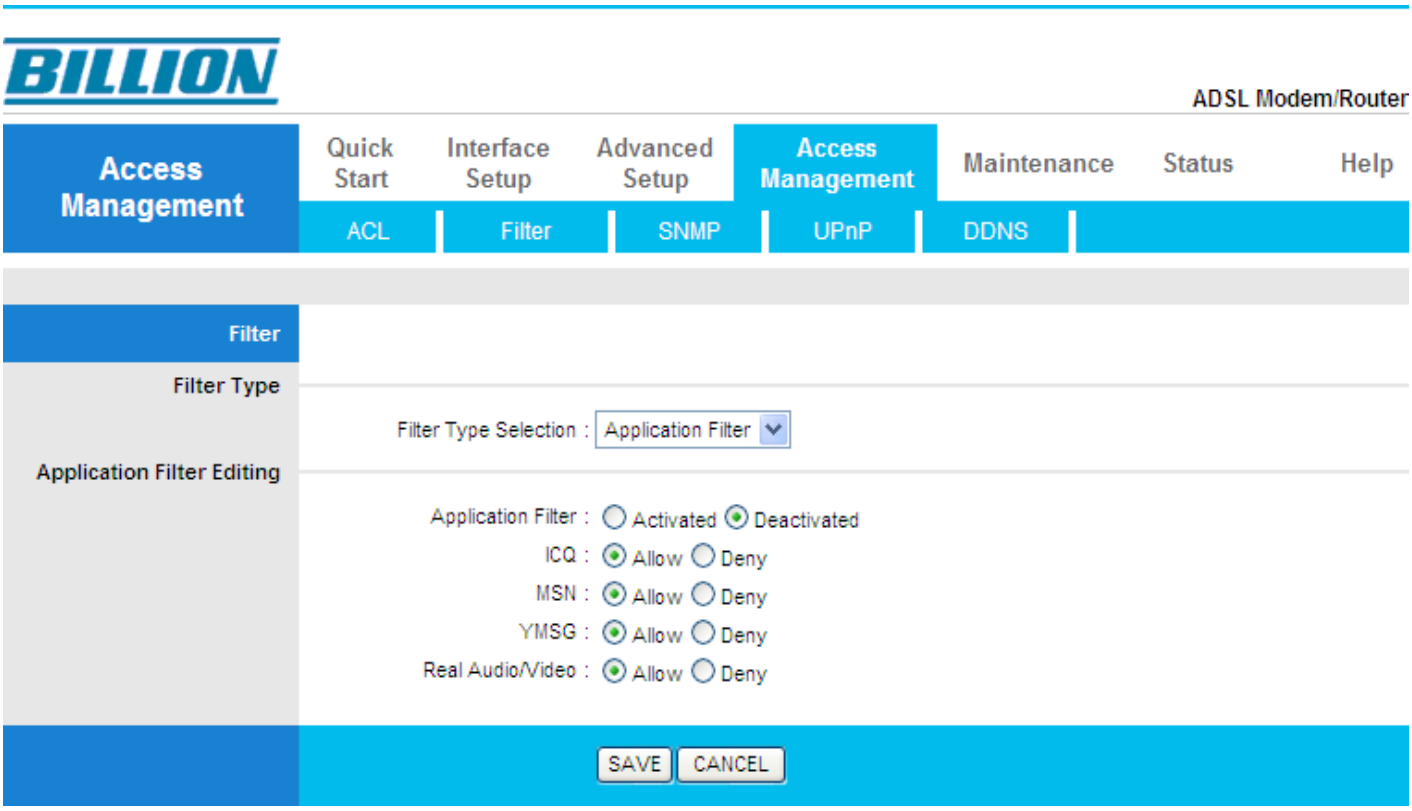
Src port: This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range 0 ~ 65535. It is recommended that this option be configured by an advanced user.

Dest Port: This is the Port or Port Ranges that defines the application.

Protocol: It is the packet protocol type used by the application, select either TCP or UDP or ICMP

Unmatched: It show this profile setting: Forward or NEXT.

Application Filter



Application Filter: Select this option to Activated/Deactivated the Application filter.

ICQ: Select this option to Allow / Deny ICQ.

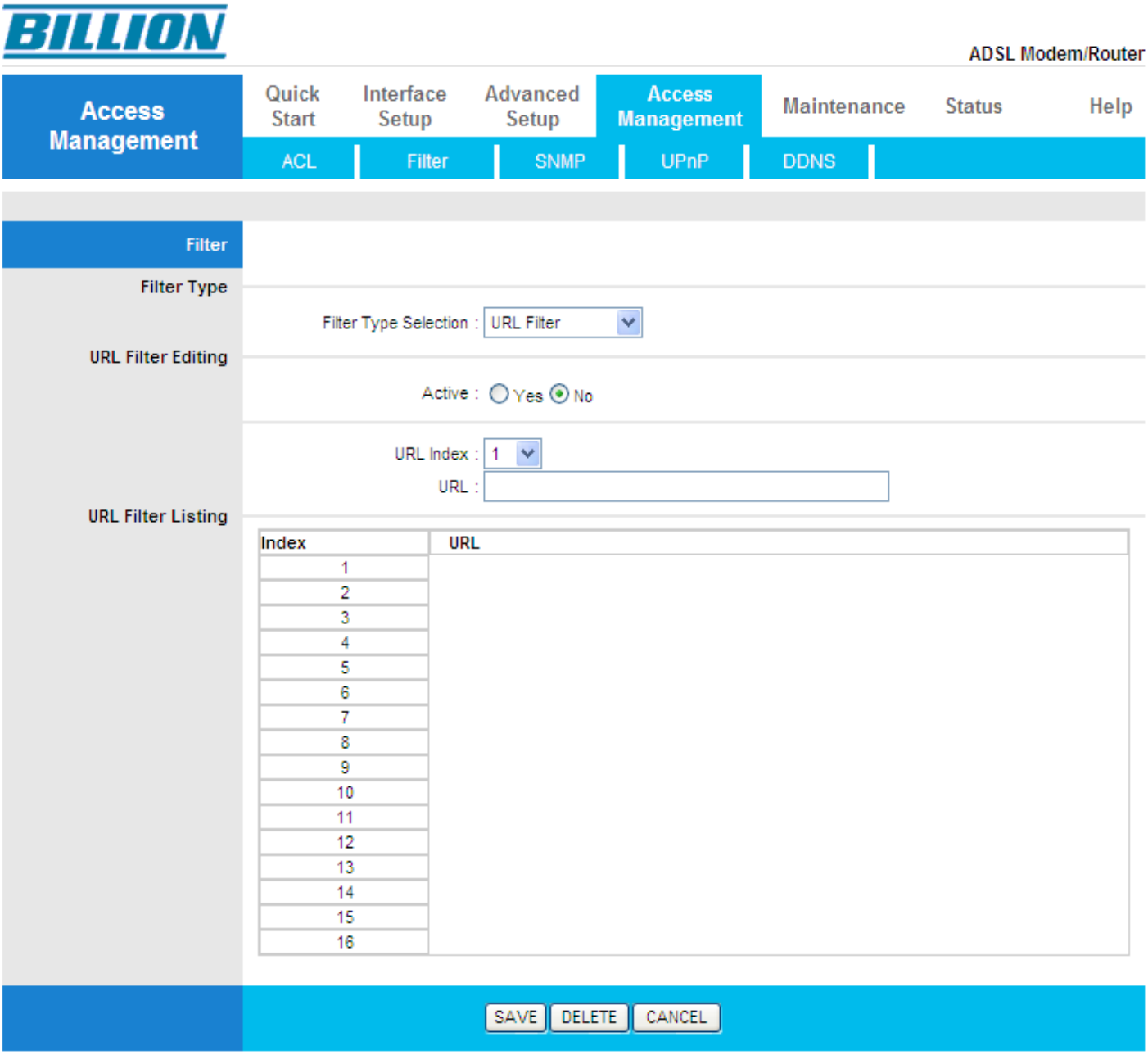
MSN: Select this option to Allow / Deny MSN.

YMSG: Select this option to Allow / Deny Yahoo messenger.

Real Audio/Video: Select this option to Allow / Deny Real Audio / Video.

Press **SAVE** to apply your settings.

URL



Active: Select Actived to enable URL Filter.

URL Index: This is item number.

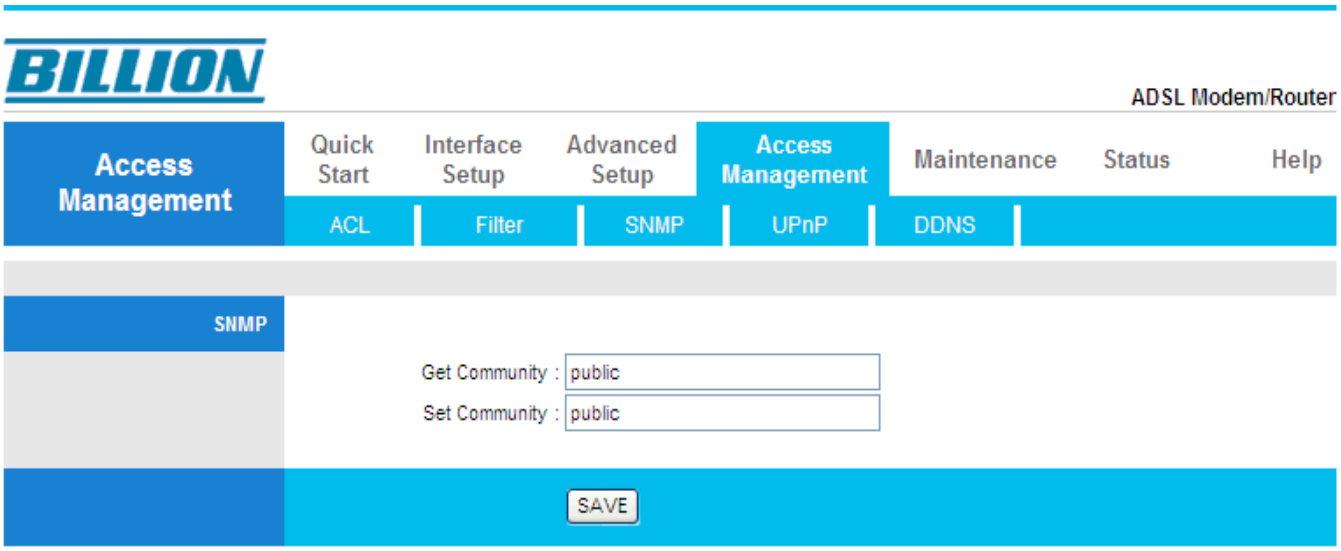
URL: Allow you to prevent users on your network from accessing particular websites by their URL.

Press **SAVE** to confirm your settings, and the corresponding settings will be listed in the **URL Filter Listing** table.

Select the rule index of the item you want to delete from the **URL Index** drop-down menu, press **DELETE** and you will delete it.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. BiPAC 5200G *RC* Series router supports SNMP agent function that enables manager station to manage and monitor the router through the network.



Get Community: Type the Get Community, which is the password for the incoming Get-and GetNext requests from the management station.

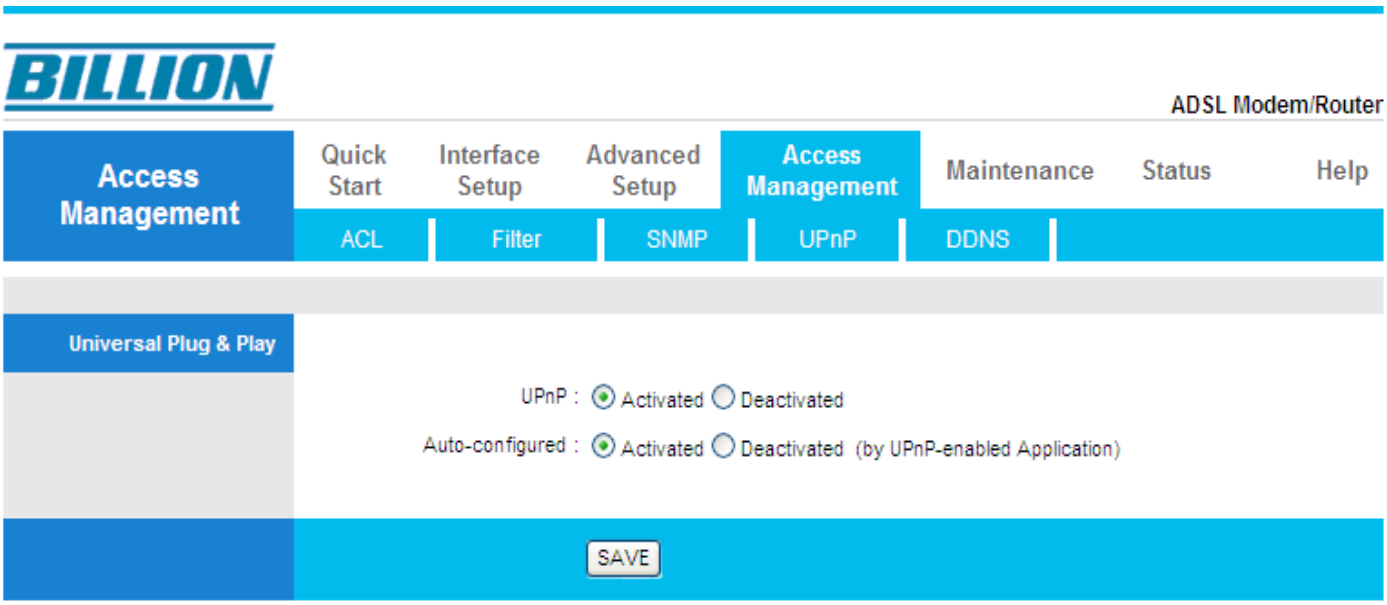
Set Community: Type the Set Community, which is the password for incoming Set requests from the management station.

Press **SAVE** to apply your settings.

UPnP

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with controlling data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal and on supported systems. Task handling such as port forwarding becomes easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows ME natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.



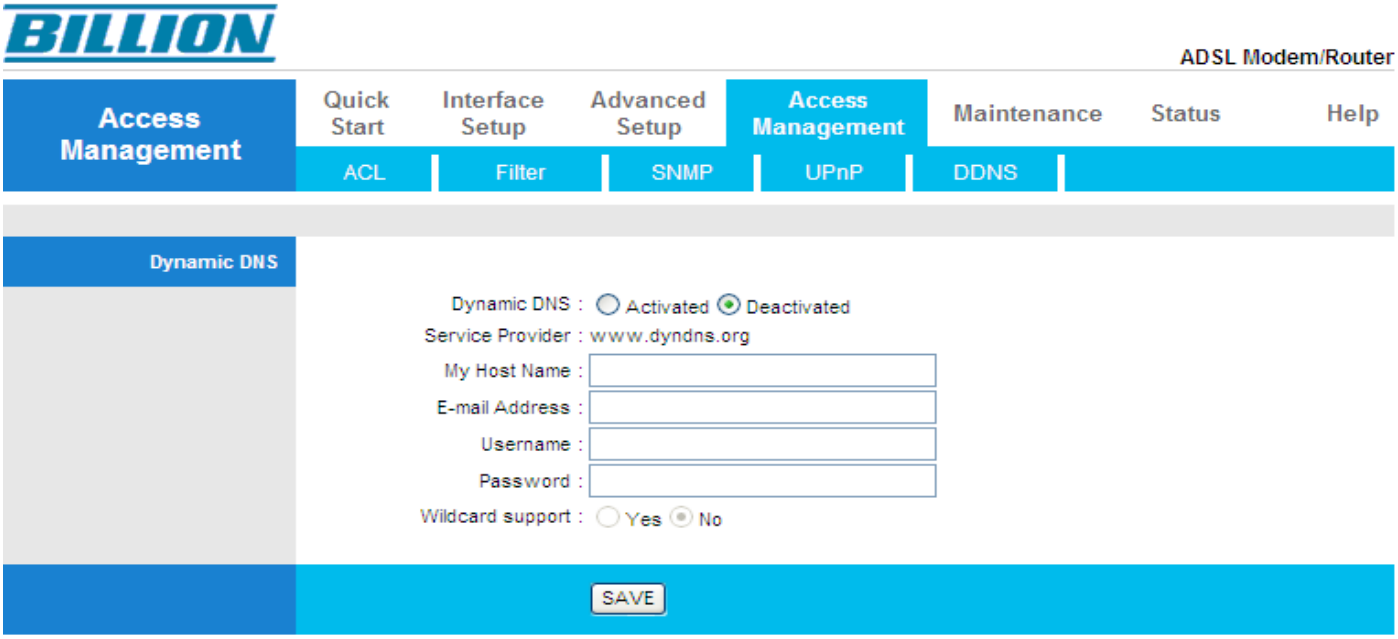
UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without having to enter the router IP address.

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure your BiPAC router so that they can communicate through the router. For example, by using NAT traversal UPnP applications will automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device. This eliminates the need to manually configure port forwarding for the UPnP enabled application.

Press **SAVE** to apply your settings.

DDNS

Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is useful when hosting servers via your ADSL connection, so that anyone wishes to connect to you may use your domain name rather than having to use your ever changing dynamic IP address. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.



Dynamic DNS: Select this check box to use dynamic DNS.

Service Provider: **www.dyndns.org**

My Host Name: Type the domain name assigned to your router by your Dynamic DNS provider.

E-mail Address: Type your e-mail address.

Username: Type your user name.

Password: Type the password assigned to you.

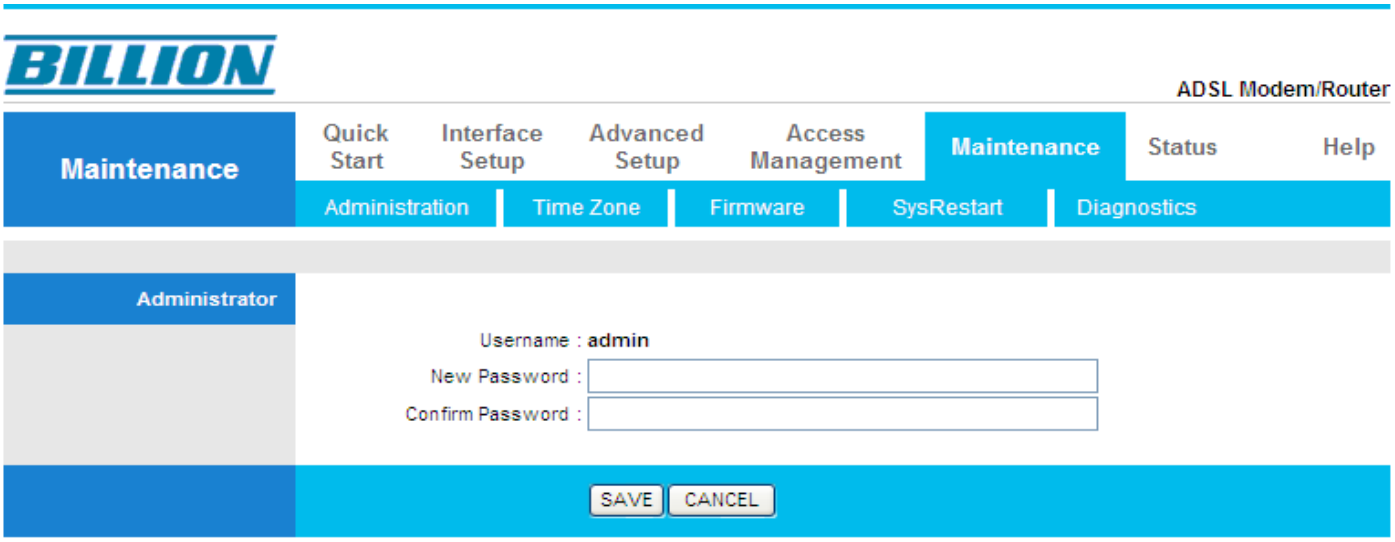
Wildcard support: Select this check box to enable DYNDNS Wildcard.

Press **SAVE** to apply your settings.

Maintenance

Administration

In default setting, the username and password are both "admin". You can change the default password to ensure that someone cannot adjust your settings without your permission. Every time you change your password, please record the password and keep it safe.



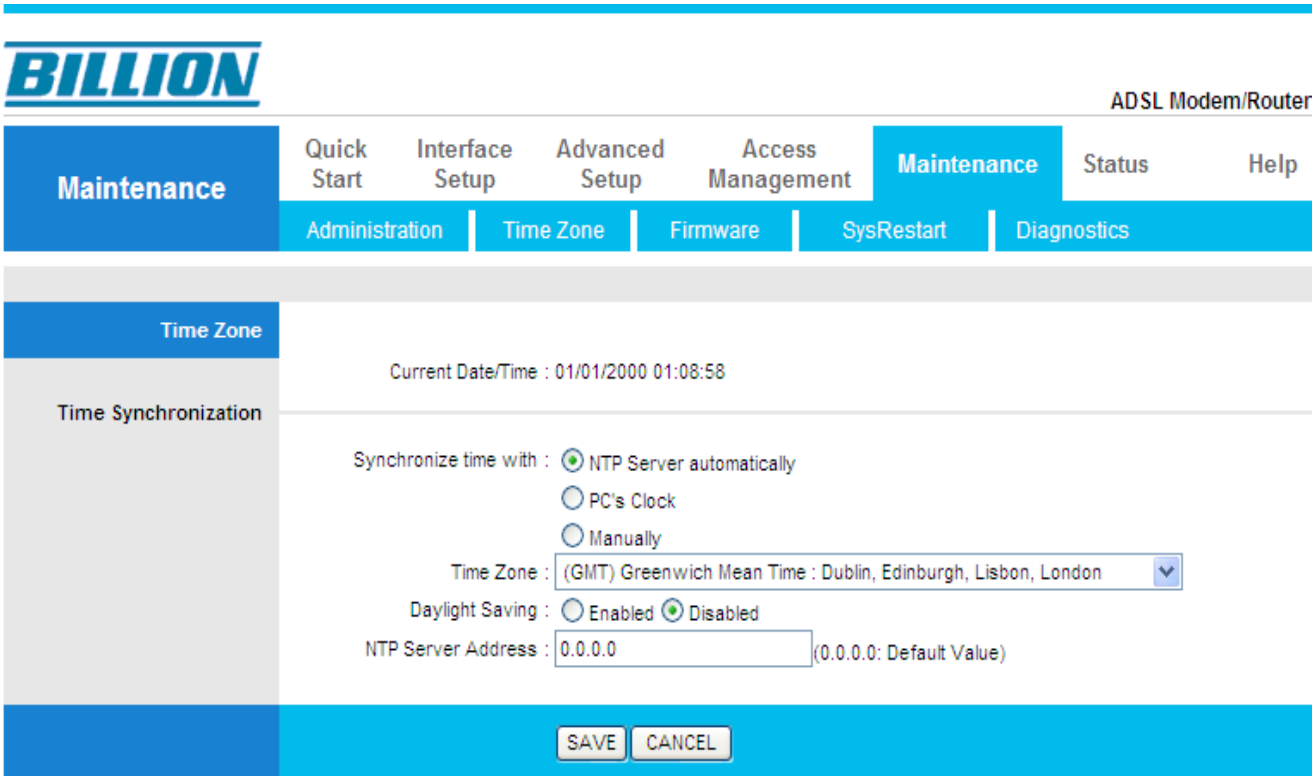
New Password: Type the new password in this field

Confirm Password: Type the new password again in this field.

Press **SAVE** to apply your settings.

Time Zone

The router does not have a real time clock onboard. Instead it gets the current time through the Simple Network Time Protocol (SNTP) from an SNTP server outside your network. Choose your local time zone. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.



Synchronize time with: Select the time service protocol that your time server sends when you turn on the Router.

Time Zone: Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

Daylight Saving: Select this option if you use daylight savings time.

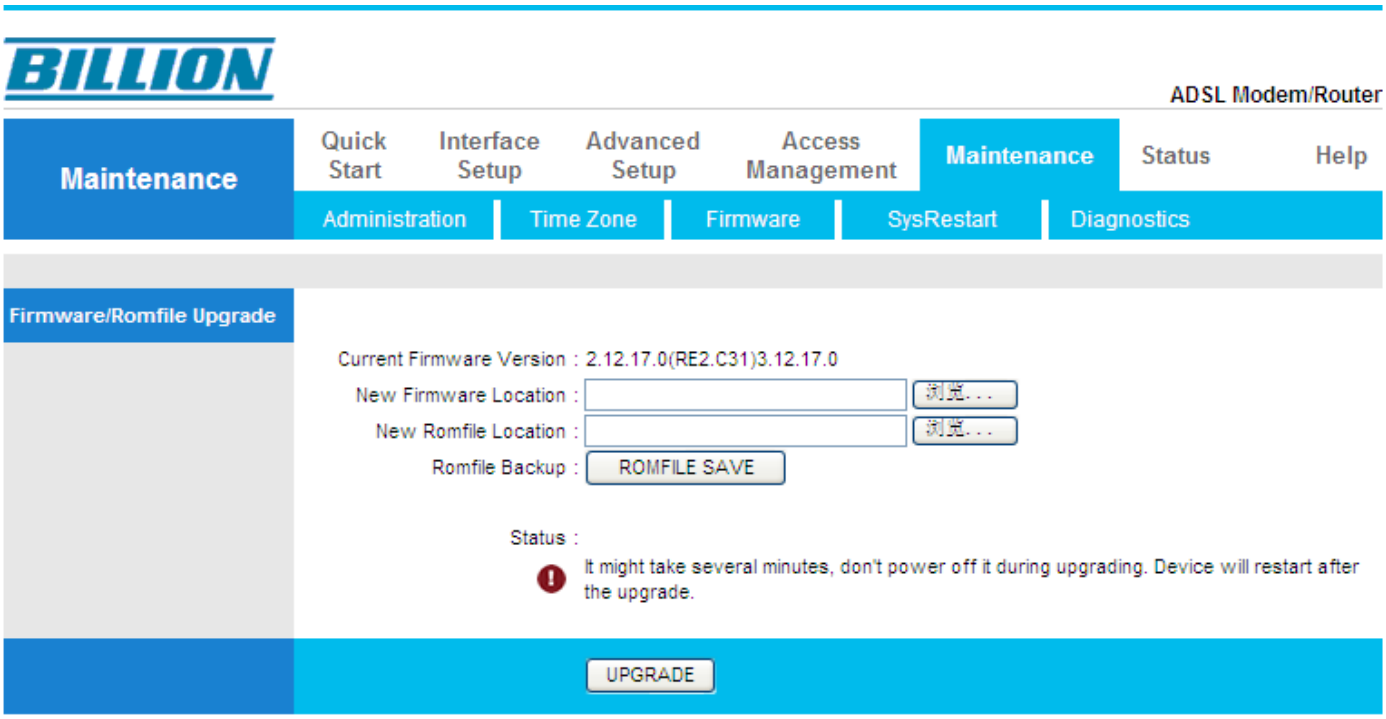
NTP Server Address: Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.

Press **SAVE** to apply your settings.

Firmware

Your router firmware is the like a software that allows your router to operate and perform all its functions. Thus, by upgrading your router to the latest firmware, you can experience the greater features and functionality that have been created.

To upgrade the firmware of your router, you should download or copy the firmware to your local environment first. Then press “Browse…” button to specify the path of the firmware file. Then, click “Upgrade” to start the upgrading process. When the procedure is completed, the router will reset automatically to apply the new firmware setting.



New Firmware Location: Type in the location of the file you want to upload in this field or click Browse to find it.

New Romfile Location: Romfile means the configuration file. Type in the location of the file you want to upload in this field or click Browse to find it.

Browse: Click Browse... to find the .ras file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.

Romfile Backup: Click ROMFILE SAVE button to save current configuration file to your PC.

UPGRADE: Click UPGRADE to begin the upload process. This process may take up to two minutes.

After two minutes, log in again and check your new firmware version on the System Status page.

If the upload was not successful, click Back to go back to the Firmware screen and repeat the process.

Warning

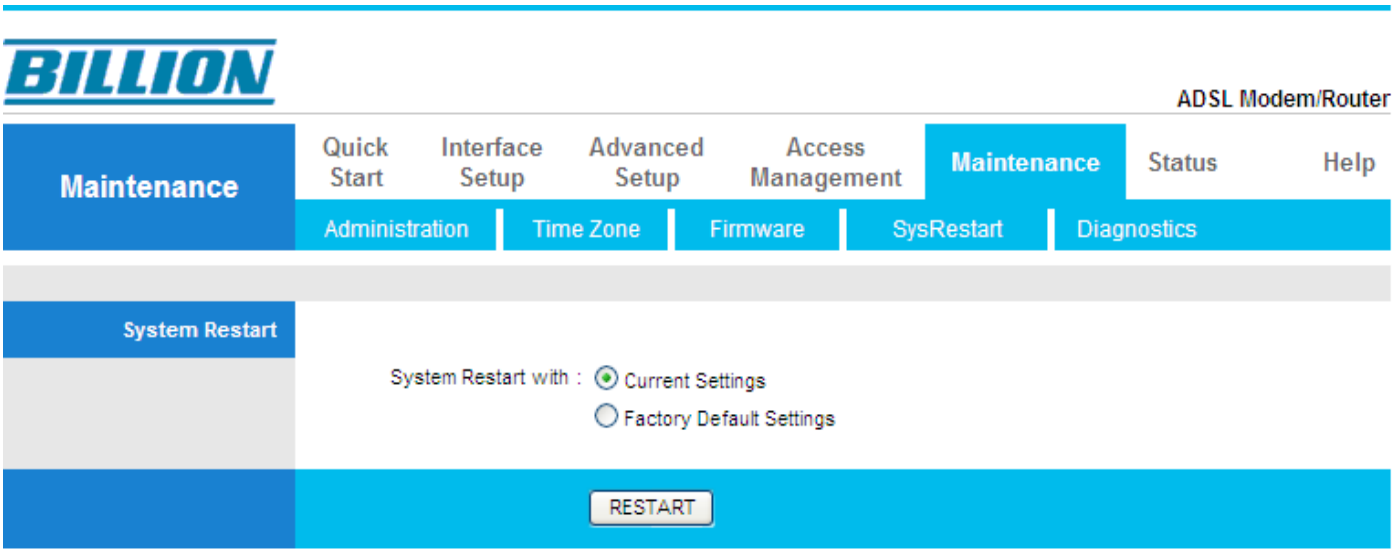
DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

SysRestart

Click SysRestart with option Current Settings to reboot your router (and restore your last saved configuration).

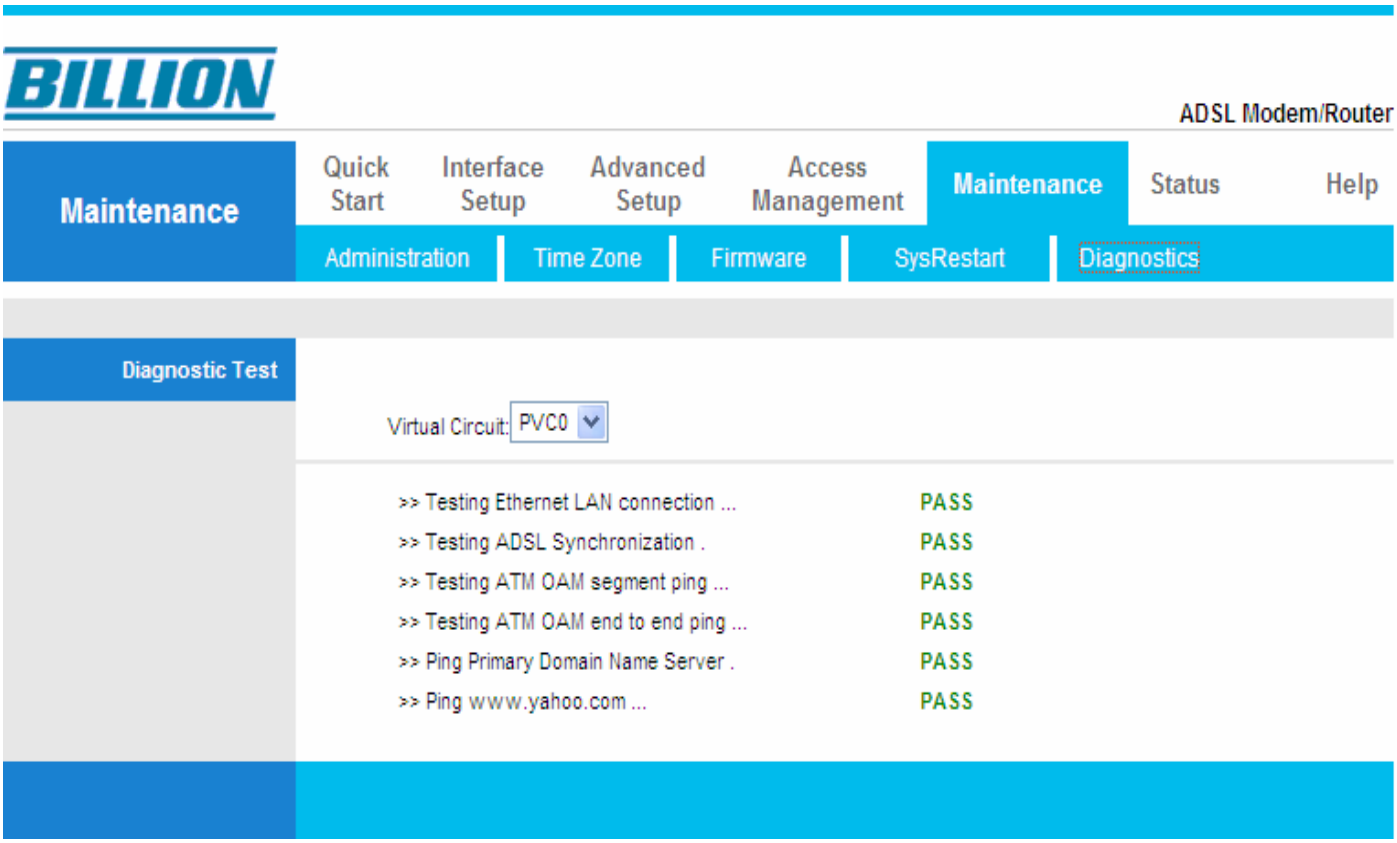
If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings.

You may also reset your router to factory settings by holding the small Reset pinhole button on the back of your router in more than 6 seconds whilst the router is turned on.



Diagnostics

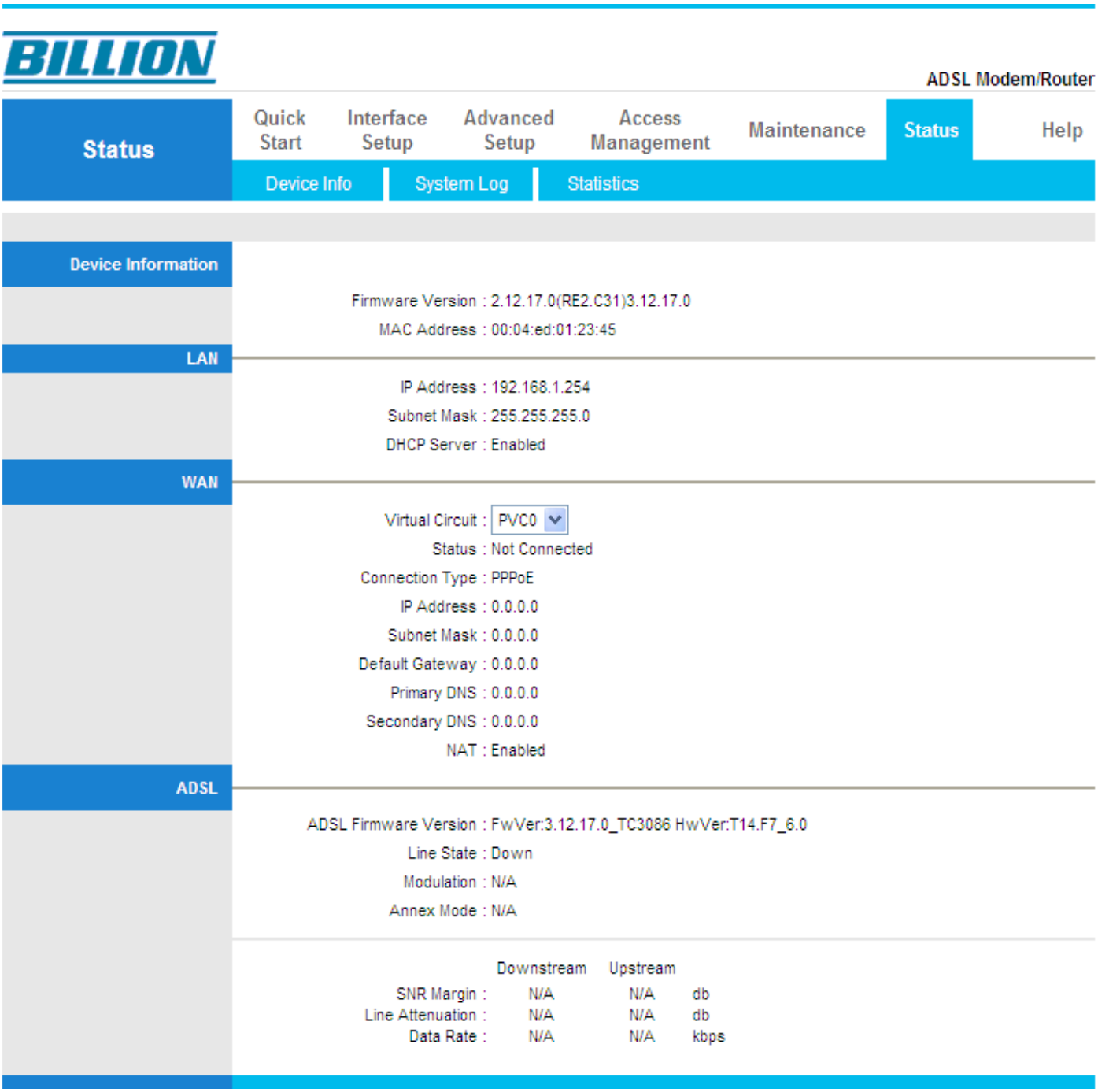
The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.



Status

Device Info

This page displays the current information for the ADSL Router. It will display the Firmware version, LAN, WAN, and MAC address information.



Device Information

Firmware version: This is the Firmware version.

MAC Address: This is the router MAC Address.

LAN

IP Address: LAN port IP address.

Sub Net Mask: LAN port IP subnet mask.

DHCP Server: LAN port DHCP role - Enabled, Relay or disabled.

WAN

Virtual Circuit: There are eight groups of PVC can be defined.

Status: “Not connected” or “Connected”.

Connection Type: Name of the WAN connection.

IP Address: WAN port IP address.

Subnet mask: WAN port IP subnet mask.

Default Gateway: The IP address of the default gateway.

Primary DNS: the address of the primary DNS server.

Secondary DNS: the address of the secondary DNS server.

NAT: Enabled or Disabled NAT function.

ADSL

ADSL firmware version: This is the DSL firmware version associated with your router.

Line State: This is the status of your ADSL link.

Modulation: This field displays the ADSL modulation status for G.dmt or T1.413.

Annex Mode: To show the router’s type, e.g. Annex A, Annex B.

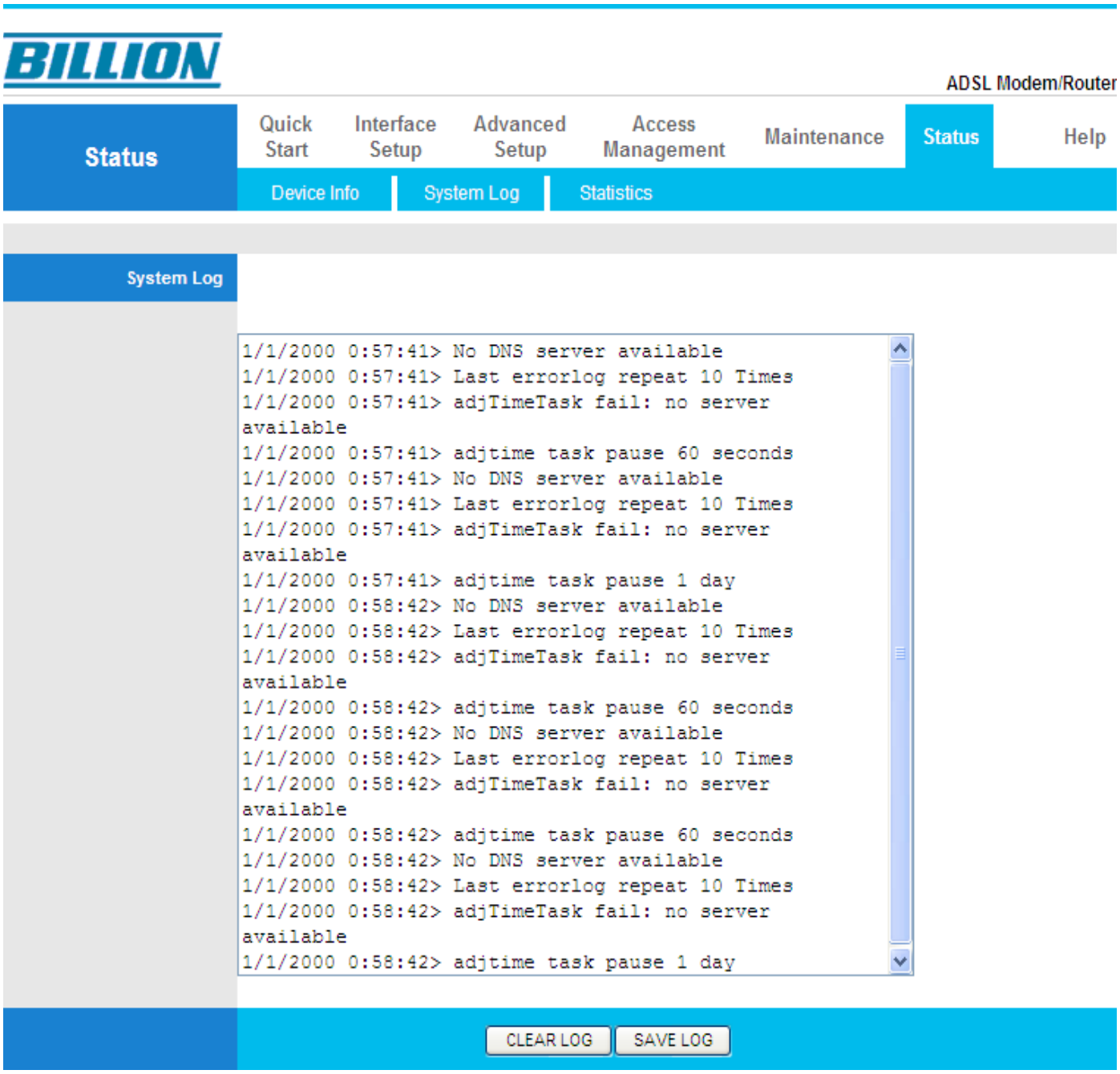
SNR Margin: To show the router’s SNR margin for Downstream/Upstream.

Line Attenuation: To show the router’s for Downstream/Upstream.

Data Rate: To show the router’s data rate for Downstream/Upstream.

System Log

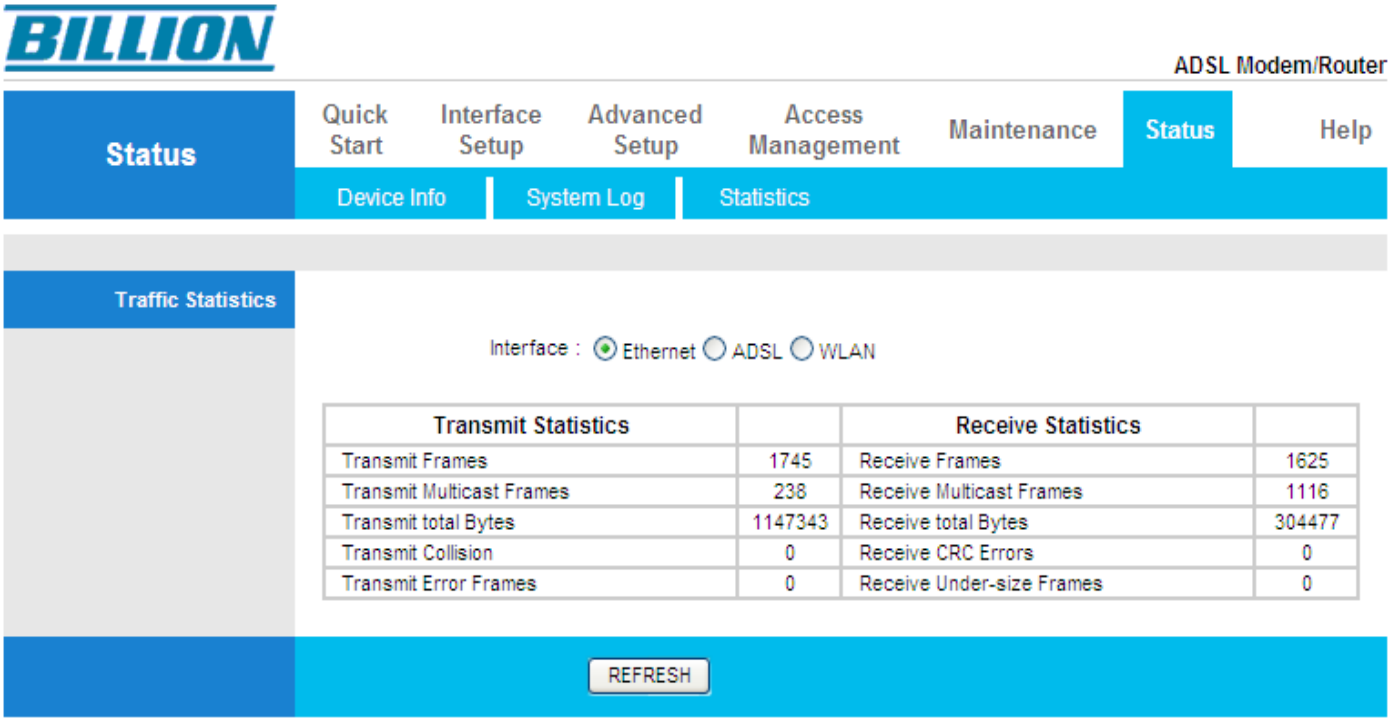
Display system logs accumulated up to the present time. You can trace historical information with this function.



Statistics

Read-only information here includes port status and packet specific statistics. Also provided are "Transmit Statistics" and "Receive Statistics".

Ethernet



Interface: This field displays the type of port.

Transmit Frames: This field displays the number of frames transmitted in the last second.

Transmit Multicast Frames: This field displays the number of multicast frames transmitted in the last second.

Transmit total Bytes: This field displays the number of bytes transmitted in the last second.

Transmit Collision: This is the number of collisions on this port.

Transmit Error Frames: This field displays the number of error packets on this port.

Receive Frames: This field displays the number of frames received in the last second.

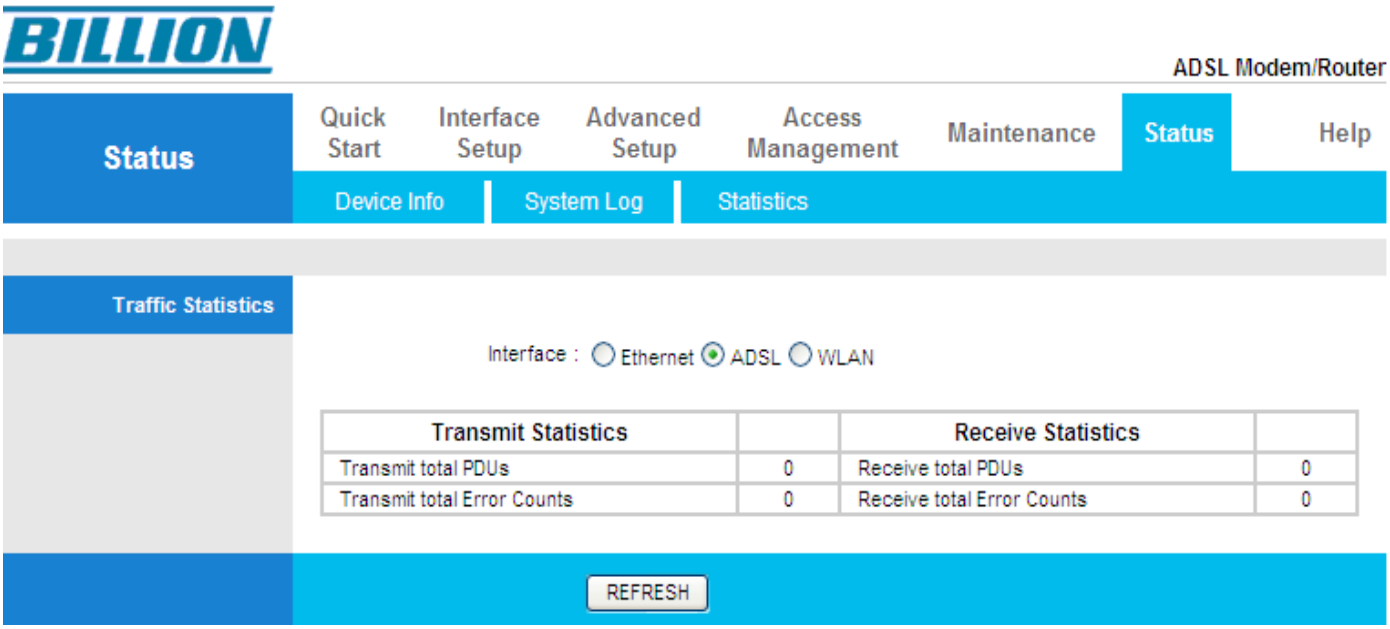
Receive Multicast Frames: This field displays the number of multicast frames received in the last second.

Receive total Bytes: This field displays the number of bytes received in the last second.

Receive CRC Errors: This field displays the number of error packets on this port.

Receive Under-size Frames: This field displays the number of under-size frames received in the last second.

ADSL



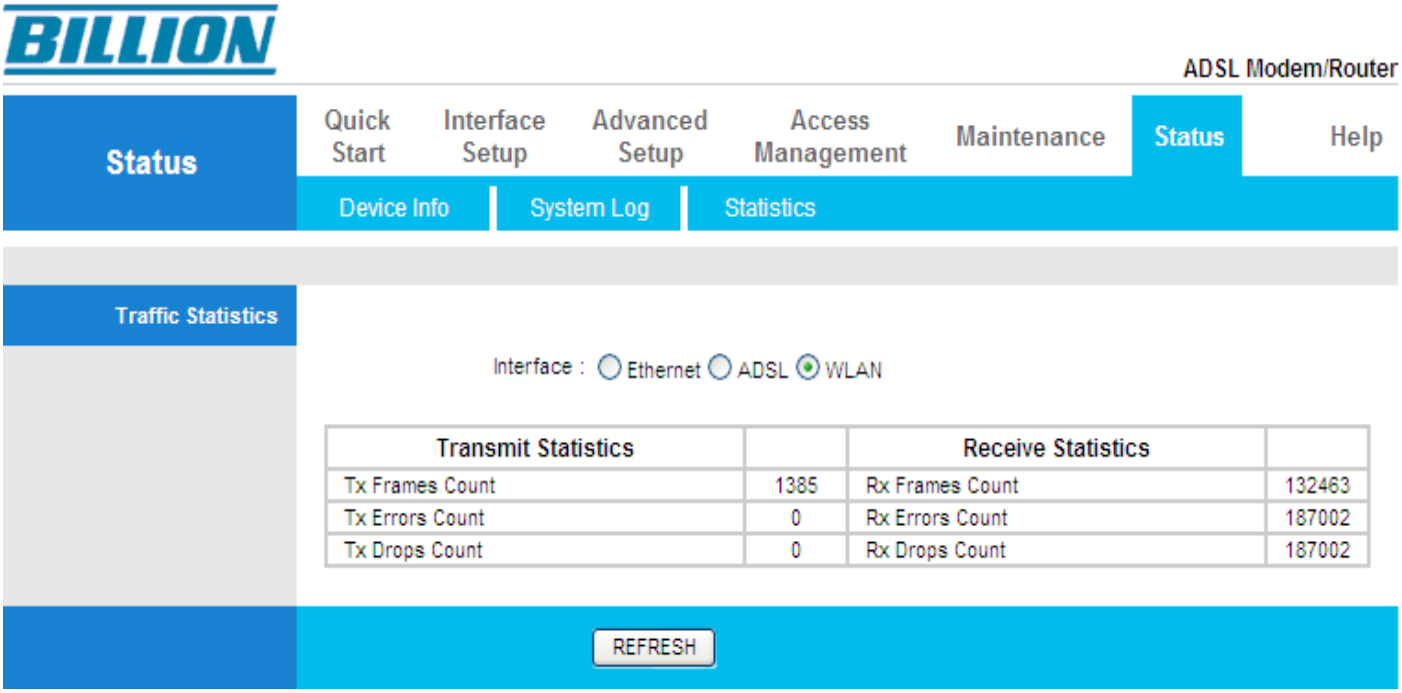
Transmit total PDUs: This field displays the number of total PDU transmitted in the last second.

Transmit total Error Counts: This field displays the number of total error transmitted in the last second.

Receive total PDUs: This field displays the number of total PDU received in the last second.

Receive total Error Counts: This field displays the number of total error received in the last second.

WLAN



Tx Frame Count: This field displays the number of frames transmitted in the last second.

Tx Errors Count: This field displays the number of errors frames transmitted in the last second.

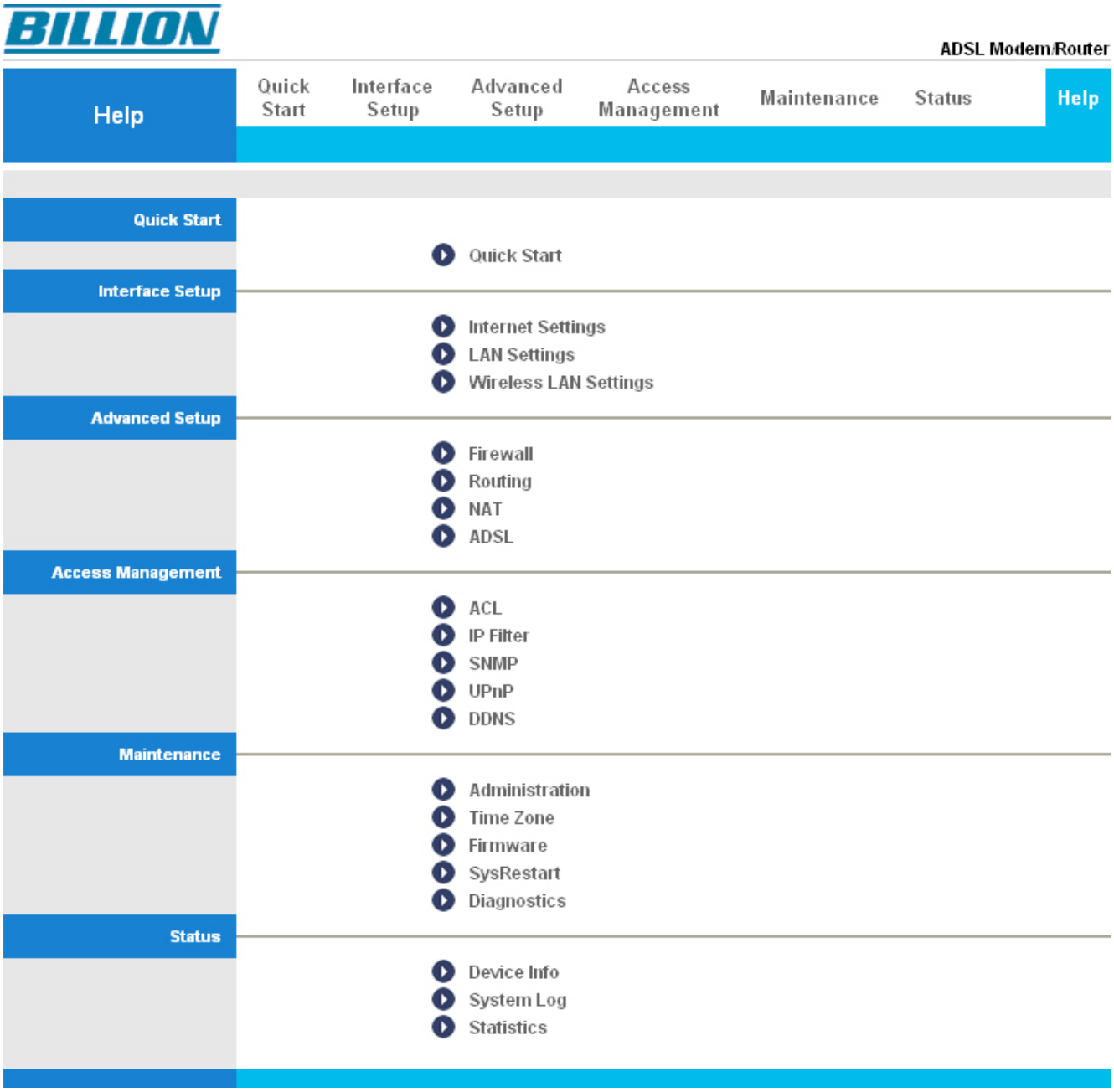
Tx Drops Count: This field displays the number of drops frames transmitted in the last second.

Rx Frames Count: This field displays the number of frames received in the last second.

Rx Errors Count: This field displays the number of errors frames received in the last second.

Rx Drops Count: This field displays the number of drops frames received in the last second.

Help



This help page provides you some useful messages such as the introductions of some concepts and some guidances.When some problems are encountered, you can turn to this page for help.
For example, if you don't understand what is Quick Start, you can go to this page, click on Quick Start, then you'll see some messages about it, and understand it quickly. This function provides you an easy way to help yourself.

Chapter 5: Troubleshooting

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or Billion for support.

Problems with the router

Problem	Suggested Action
None of the LEDs lit when the router is turned on.	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
You have forgotten your login username or password	Try the default username “admin” and password “admin”. If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router more than 6 seconds.

Problems with WAN interface

Problem	Suggested Action
Initialization of PVC connection (line sync) fail	Make sure that the telephone cable is properly connected between the ADSL port and the wall jack. The ADSL LED on the front panel should lit. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router GE. If you still have problem, you may need to verify these settings with your ISP.
Frequent loss of ADSL line sync (disconnection)	Make sure that all devices (e.g telephone, fax machine, analogue modems) that are connected to the telephone line as your router have a line filter connected between them and the wall outlet (unless your are using a Central Splitter or Central Filter installed by a qualified and licensed electrician). Make sure that alll line filters are correctly installed as missing line filters or incorrect installation of line filters can cause ADSL connection problem, including frequent disconnections.

Problem with LAN interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

Appendix: Product Support & Contact

Following the suggestions listed in the Troubleshooting section of the user manual can help you solve most of your problems. However if your problems persist or you come across other technical issues that are not listed in the Troubleshooting section, please contact the dealer from where you purchased your product.

Contact Billion

Worldwide:

http://www.billion.com

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/98, Windows NT, Windows 2000, Windows Me, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.